

**LA LOPD:**  
**LEY ORGÁNICA DE PROTECCIÓN**  
**DE DATOS**

Gago Figueroa, Elías  
Ramos Rodríguez, Javier  
González González, Emilio

## ÍNDICE

Introducción	pág. 3
Historia de la Lopd	pág. 7
Análisis Lopd	pág. 10
Diferencias Lopd – Lortad	pág. 24
Leyes en otros países	pág. 28
Delitos Informáticos	pág. 32
Auditoría	pág. 44
Conclusión	pág. 54
Bibliografía	pág. 55

## INTRODUCCIÓN

La nueva Ley de Protección de Datos de Carácter Personal (Ley Orgánica 15/1999, de 13 de diciembre).

El pasado 14 de enero de 2000 entró en vigor en España la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) que ha derogado la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (la conocida como LORTAD) hasta esa fecha vigente en nuestro país.

La aprobación de esta nueva Ley ha vuelto a plantear en España el debate sobre cuál debe ser el punto de equilibrio entre la protección de la privacidad de los ciudadanos y los legítimos intereses de todos aquellos que precisan de datos de carácter personal para el -desarrollo de sus actividades. Lamentablemente, no parece que la nueva ley española vaya a servir para asegurar el equilibrio de los intereses en juego que exige la Directiva 95/46/EC por lo que, desde nuestro punto de vista, se ha perdido la gran oportunidad de mejorar y corregir las deficiencias que supuso la LORTAD de 1992.

El ámbito de aplicación de la nueva Ley se amplía a todos los ficheros de datos, informatizados o no. De la misma forma que el art. 32.2 de la Directiva, la disposición adicional primera de la LOPD establece el plazo de 12 años a contar desde el 24 de octubre de 1995 para que los ficheros y tratamientos no automatizados se adecuen a los mandatos de la nueva Ley.

El art. 2.1 delimita más claramente el ámbito de aplicación territorial de la Ley estableciendo, entre otros extremos, que se regirán por la Ley española aquellos tratamientos en los que al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de las normas de Derecho Internacional Público, y aquellos en los que el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

La Ley de 1992 sólo recogía la figura del responsable del fichero. Con la nueva Ley se introduce la figura del encargado del tratamiento que se define de la misma forma que en el art. 2.e) de la Directiva 95/46/EC. Debe tenerse en cuenta que el encargado del tratamiento debe adoptar las medidas de seguridad que le sean exigibles y está sujeto a responsabilidad pudiendo ser sancionado por la Agencia de Protección de Datos (hasta ahora sólo se podía sancionar a los responsables de los ficheros).

En el sistema español uno de los supuestos de excepción al principio del consentimiento exigido para el tratamiento de los datos es aquél en el que los datos figuren en fuentes accesibles al público. Pues bien, frente a la definición enunciativa y no limitativa de fuentes accesibles al público que existía en España, la nueva Ley limita las fuentes accesibles al público exclusivamente al censo promocional al que nos referiremos más adelante, los repertorios telefónicos, listados de profesionales colegiados, diarios y boletines oficiales y los medios de comunicación.

El que las fuentes accesibles al público pasen, con la nueva Ley, a ser un *numerus clausus* va a suponer grandes problemas, sobre todo para las empresas del sector del marketing y la publicidad directa que para desarrollar sus actividades deben utilizar datos que figuren en fuentes accesibles al público o bien datos facilitados por los propios interesados u obtenidos con su consentimiento.

La Ley española dedica su Título II (artículos 4 a 12) a los denominados principios de protección de datos. Las novedades más destacables que se introducen en este Título de la Ley son las siguientes:

La nueva Ley, más en línea con lo establecido en el art.6.1.b) de la Directiva, establece que los datos objetos de tratamiento no podrán usarse para finalidades incompatibles (la Ley de 1992 decía distintas) con aquellas para las que los datos hubieran sido recogidos.

Esta modificación del principio de finalidad soluciona muchos problemas prácticos que se habían planteado hasta la fecha.

El art. 5.4 LOPD introduce la regulación del derecho de información cuando los datos no han sido recabados del propio interesado de igual forma que en el art. 11 de la Directiva.

Se introduce en la normativa española el derecho de oposición regulado en el artículo 14 de la Directiva de una forma bastante defectuosa ya que no se le dedica un artículo independiente sino que se introduce en el artículo en el que se regula el principio del consentimiento y sus excepciones.

El artículo 7 LOPD, a diferencia de la Ley de 1992, incluye entre los denominados datos especialmente protegidos los datos relativos a la afiliación sindical, cumpliendo, de esta forma, con lo establecido en el artículo 8 de la Directiva.

Por último, se introduce un nuevo artículo 12 (acceso a los datos por cuenta de terceros), que tiene como antecedente el art. 27 de la Ley de 1992 y que se inspira en el artículo 17.3 de la Directiva según el cual no se considera cesión de datos el acceso a los datos de un tercero cuando dicho acceso es necesario para la prestación de un servicio al responsable del tratamiento. Este artículo vendrá a solucionar muchos problemas suscitados con ocasión de la prestación de servicios de outsourcing.

A pesar de la multitud de críticas que ocasionó el distinto régimen existente entre los ficheros de titularidad pública y los de titularidad privada en la LORTAD (que no encuentra justificación en la Directiva) la nueva Ley sigue manteniendo esta distinción que, entre otros extremos, implica un distinto régimen sancionador que supone que las infracciones de los responsables de los ficheros de titularidad pública no son castigadas necesariamente con multa.

Movimiento internacional de datos La nueva Ley, como la Ley de 1992, exige que para que se pueda llevar a cabo una transferencia temporal o definitiva de datos con destino a países que no proporcionen un nivel de protección equiparable al de la Ley española se cumpla con los mandatos de la Ley y, además, se obtenga una autorización previa del Director de la Agencia de Protección de Datos.

Sin embargo, en contraste con la Ley de 1992, la LOPD mejora, en sus artículos 33 y 34, la regulación del movimiento internacional de datos y transpone las reglas establecidas en los artículos 25 y 26 de la Directiva que, tanta importancia tienen en nuestra globalizada economía.

Frente a la confusa regulación que existía en España en relación con las transferencias de datos dirigidas a otros países de la Unión Europea, el nuevo art. 34 k) establece, que no es necesario obtener autorización previa del Director de la Agencia de Protección de Datos cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado. En este sentido, a la luz de las disposiciones de la Directiva y de las propias normas del Tratado de Roma, debe tener el mismo tratamiento una transferencia de datos entre Madrid y Barcelona que una transferencia realizada entre Madrid y Londres por lo que la única prevención antes de realizar este tipo de operaciones entre países de la Unión será cumplir con las normas generales sobre comunicación o cesión de datos que establece el artículo 11 LOPD.

El problema se sigue suscitando con las transferencias internacionales de datos a Estados Unidos que, no proporciona un nivel de protección equiparable al español. De hecho, la mayor parte de los expedientes de autorización previa de transferencias internacionales de datos tramitados por la Agencia de Protección de Datos han tenido como país de destino de los datos a Estados Unidos.

La autoridad de control (art. 28 de la Directiva) española es la Agencia de Protección de Datos configurada, desde la Ley de 1992, como un órgano que actúa con plena independencia de las Administraciones Públicas, controlador y fiscalizador de la aplicación de la Ley y con capacidad investigadora y sancionadora. La Agencia está dirigida y representada por un Director con amplísimos poderes según la legislación española. Hubiera sido deseable, que la nueva Ley hubiese aprovechado para dar a la Agencia de Protección de Datos una orientación colegiada para acabar con la concentración de poder en sola persona (el Director).

Es este uno de los puntos que permite afirmar que la aprobación de la nueva Ley es la historia de una oportunidad perdida ya que se ha desaprovechado la oportunidad de limitar los excesivos poderes concentrados en una sola persona, el Director de la Agencia, lo que hubiera permitido adoptar fórmulas para que éste hubiese precisado de las opiniones de otras personas antes de adoptar sus resoluciones evitando, así, posturas extremas.

Este es otro de los aspectos de la nueva Ley en los que se ha desaprovechado la oportunidad de enmendar los errores de la LORTAD de 1992. La nueva Ley introduce algunas modificaciones como la extensión del régimen de responsabilidad no sólo a los responsables de los ficheros sino también a los encargados de los tratamientos, otra mejora es la mejor tipificación de determinadas infracciones, asimismo también debe destacarse que la nueva Ley introduce en el art.45.5 la posibilidad de que se rebaje la cuantía de las sanciones en supuestos de cualificada disminución de la culpabilidad o de la antijuridicidad del hecho.

Sin embargo, decimos que este es otro ejemplo de oportunidad perdida por la nueva Ley ya que ésta mantiene las absolutamente desproporcionadas y desmesuradas cuantías de las multas. Así las infracciones leves se siguen sancionando con multa de 601,01€ a

60.101,21€ (100.000 a 10.000.000 de pesetas) las infracciones graves con multa de 60.101,21€ a 300.506,05€ (10.000.000 a 50.000.000 de pesetas) y las infracciones muy graves con multa de 300.506,05€ a 01.012,010€ (50.000.000 a 100.000.000 de pesetas).

La desmesurada cuantía de estas multas hace de España el país con el régimen sancionador más duro de toda la Unión Europea y, desde nuestro punto de vista, coloca a las empresas españolas en una situación de desigualdad frente a sus competidores europeos. De hecho, tan desmesuradas multas van en contra del espíritu de la Directiva que en entre sus objetivos buscaba que se eliminasen las diferencias entre los niveles de protección de la privacidad de las personas en los Estados Miembros para no obstaculizar el ejercicio de una serie de actividades económicas a escala comunitaria.

## HISTORIA

*<<Sólo un poder que disponga de informaciones apropiadas podrá favorecer el desarrollo y garantizar la independencia de un país>>.  
(La informatización de la sociedad)*

La protección de los datos de carácter personal comienza en Europa en el año 1970 en el Land de Hesse de la República Federal Alemana (Datenschutz de 7 octubre de 1970) que posteriormente sería modificada en 1978 y 1986.

Posteriormente fueron apareciendo leyes sucesivas en la mayoría de los países Europeos. Las diferentes leyes podemos dividirlos en tres generaciones que responden a tres parámetros diferenciadores:

- 1.-Evolución de los propios derechos fundamentales de las personas.
- 2.-Innovaciones Tecnológicas
- 3.-Adaptación de las leyes de protección de datos a la nueva situación creada.

La primera generación trata de establecer unos límites en el uso de la informática, dado el gran avance que se produjo en este campo fueron necesarias la creación de diferentes leyes a lo largo de estos últimos años. El cambio en nuestros estilos de vida, en nuestros hábitos, los cambios en la economía, en la política, etc. También han influenciado en la aparición de nuevas leyes. La información se ha convertido en el arma más poderosa en un país y la creación de leyes que la controlen ha sido necesaria.

La segunda generación trataba de asegurar la calidad de los datos. Cada año aparecen tecnologías nuevas que manejan cada vez una mayor cantidad de información y es necesario que surjan leyes que controlen su calidad y fiabilidad.

La tercera generación defiende la autodeterminación informática y la libertad informática.

En nuestro país el origen de la protección de datos comienza con la Constitución de 6 de diciembre de 1978.

### CONSTITUCIÓN ESPAÑOLA

El título primero de la constitución española de 6 de diciembre de 1978( “De los derechos y deberes fundamentales”) es sin duda uno de los más largos e importantes de la constitución. En la sección 1ª del capítulo segundo trata de los derechos fundamentales y las libertades públicas.

Cobra especial importancia el artículo 18. Intimidad. Inviolabilidad de domicilio. Especialmente el punto 4.

<<Artículo 18(Derecho a la Intimidad, Inviolabilidad de domicilio).

1.- Se garantizará el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2.- El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3.- Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4.- La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.>>

Por lo tanto el fin de la LORTAD era poner freno a lo que entendían los redactores de la Constitución era un peligro para la defensa de la intimidad de los ciudadanos: la implantación cada día mayor en nuestra sociedad de la nuevas tecnologías de la información, especialmente a partir del enorme avance experimentado por las comunicaciones.

Pasaron catorce años desde la promulgación de la Constitución hasta que se desarrolló del artículo 18.4 una Ley Orgánica, ésta ley orgánica sería conocida como la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos(LORTAD) que fue puesta en marcha en el año 1992 y fue el paso mas grande llevado a cabo por España de cara a la protección de datos.

## LA LORTAD

El motor impulsor de esta ley fue sin duda el artículo 18 de la constitución pero también influyeron otros documentos anteriores a la ley que fueron propuestos en Europa:

1.-**Convenio 108 del Consejo de Europa** para la protección de las personas con respecto al tratamiento automatizada de datos de carácter personal. Fue aprobado el 28 de enero de 1981 en Estrasburgo. El convenio reconoce las necesidad del respeto a la vida privada pero asimismo la importancia de la libre circulación de la información entre los pueblos, sin tener en cuenta las fronteras. Es decir, proponía un equilibrio entra el respeto a la vida privada y la libre circulación de la información entre pueblos.

2.-**Acuerdo de Schengen** establecido el 14 de junio de 1985 entre Bélgica, Holanda, Luxemburgo, Francia y la antigua República Federal Alemana. Al acuerdo se adhirieron mas tarde España, Portugal y Grecia. Este acuerdo trataba de coordinar las políticas de asilo y acogida de emigrantes y tenían entre sus objetivos la supresión de controles en las fronteras interiores de los países firmantes del acuerdo y la libre circulación de personas entre los países. Para el logro de estos objetivos era necesario un continuo intercambio de información entre los diferentes países y asimismo la existencia de una base de datos que centralizase y almacenase dicha información.

Fruto de esta necesidad fue la creación del Sistema de Información de Schegen.

La fiabilidad de la información era esencial para un buen funcionamiento del sistema. Cada país debía adoptar disposiciones nacionales necesarias para conseguir un nivel de protección de datos de carácter personal que sea al menos, igual al resultante de los principios del Convenio del Consejo de Europa de 18 de enero de 1981 para la protección de las personas.

Se Obligaba a los países firmantes del acuerdo a tener una ley de protección de datos de carácter personal. Este acuerdo fue el principal motor inductor de la publicación de la LORTAD.

Mas tarde en marzo de 1993 aparecería la Agencia de Protección de Datos como un organismo independiente que se encarga de garantizar el cumplimiento de las previsiones y mandatos establecidos en la LORTAD.

Las funciones de la Agencia son: inspectora, ordenadora, reguladora, sancionadora, unificadora, inmovilizadora y relaciones publicas.

La LORTAD sólo estuvo en vigencia 7 años en el régimen jurídico español.

El 13 de diciembre de 1999 se procedió a la transposición a nuestro ordenamiento de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, viendo la luz de este modo la vigente Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, conocida como LOPD.

La Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) tiene un ámbito de aplicación mas amplio que la LORTAD, ya que no se limita al soporte digital exclusivamente, sino a todo tipo de soportes físicos en los que se puedan almacenar ficheros de datos. La LOPD se divide en siete títulos y una parte final compuesta por: seis disposiciones adicionales, tres disposiciones transitorias, una disposición derogatoria y tres disposiciones finales.

## ANÁLISIS DE LA LOPD

### PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Este apartado de la LOPD (artículos 4 a 12) constituye la base en el tratamiento de datos de carácter personal centrándose en los aspectos relacionados con la manipulación y gestión de la información de un modo general y exponiendo una serie de principios básicos que deberán ser contemplados por cualquier ente, público o privado, que desee manipular información de carácter personal.

### CALIDAD DE LOS DATOS

El artículo 4 proporciona unas directrices fundamentales sobre la calidad de los datos. Estas directrices van dirigidas hacia el tratamiento legal de los datos obligando a que los datos sean pertinentes, adecuados y no excesivos en relación con el ámbito y finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

Se pueden destacar los siguientes puntos:

- Los datos de carácter personal se podrán recoger para un uso adecuado, y siempre que no sobrepasen la información necesaria para la finalidad a la que sirven. Además, no se podrán usar para un fin distinto al inicialmente propuesto y serán eliminados cuando este fin haya sido alcanzado y no sea necesario su mantenimiento.
- Todos los datos almacenados deberán ser exactos, y en caso de que no lo fueran podrán ser cancelados y sustituidos por los datos rectificados sin perjuicio del afectado.
- Por último, destacar el último punto de este artículo, en el que se dice, textualmente: “Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos”. Cabe destacar que este tipo de actos están recogidos en la ley como faltas muy graves.

### INFORMACIÓN EN LA RECOGIDA DE DATOS

El titular del fichero tiene la obligación de informar al afectado cuando se recaban los datos, para que éste pueda conocer quién, cómo y para qué se tratan sus datos. Para esto el interesado debe ser informado antes de que se traten sus datos de los siguiente :

- La existencia del fichero de tratamiento de datos, de la obligatoriedad de contestar a las preguntas del formulario, de las consecuencias de no suministrarlos, de la posibilidad que tiene de cancelar y modificar estos datos y de la identidad del responsable de este fichero de datos.
- En el caso de que los datos no hayan sido directamente pedidos al interesado la empresa tiene el deber de comunicárselo al usuario en un plazo máximo de 3 meses desde su inclusión en el registro de datos. Esto no se contempla cuando los

datos sirvan para fines históricos, científicos o estadísticos, ni en el caso de datos públicos (nombre, dirección) que puedan ser usados para publicidad. En este último caso tan solo se le informará al interesado de sus derechos y del origen de los datos cuando reciba dicha publicidad.

### CONSENTIMIENTO DEL INTERESADO

El consentimiento es el principio fundamental para cualquier tratamiento de datos. Sin él no se consideraría lícito la posesión de esos datos para ser tratados en la mayoría de los casos. Si el interesado ha dado su consentimiento tendrá acceso a la información sobre el tratamiento de sus datos para conocer que es lo que se hace con ellos.

El afectado debe dar su consentimiento inequívoco al tratamiento de sus datos salvo que la ley revoque estos derechos, por ejemplo, en el caso de que los datos sean necesarios para las funciones de las Administraciones Públicas, o sean datos de carácter público. De todas formas el interesado podrá revocar el consentimiento que ha otorgado sobre sus datos si tiene causa justificada para ello y en el caso de que no haga falta darlo podrá oponerse al tratamiento de sus datos si puede justificar alguna causa que lo excluya.

### DATOS ESPECIALMENTE PROTEGIDOS

Existe una categoría de datos que la LOPD denomina “especialmente protegidos” y que son aquellos datos a los que la norma otorga un mayor grado de protección, imponiendo especiales obligaciones respecto de los mismos, tales como la necesidad de obtener el consentimiento expreso, y en su caso por escrito. Estos datos se extraen como conclusión de algunos apartados de la Constitución donde se dice que nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Los siguientes puntos detallan más claramente el trato que la ley le da a este tipo de datos:

- Solo se podrán tratar los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias con el consentimiento expreso y por escrito del afectado. Las entidades sin ánimo de lucro cuyo fin sea político, religioso, filosófico o sindical están exentas de este requisito.
- Con respecto a los datos sobre salud, raza o vida sexual solo podrán ser tratados cuando el afectado consienta expresamente, cuando la ley así lo disponga o cuando sean datos necesarios para el tratamiento médico.
- De cualquier modo, queda expresamente prohibido por la ley crear ficheros cuya única finalidad sea la de recabar información sobre ideologías, afiliaciones sindicales, religión, creencias, origen racial, o vida sexual.

### SEGURIDAD DE LOS DATOS

Como es un tema muy importante se tratará con más profundidad más adelante en este trabajo.

## COMUNICACIÓN O CESIÓN DE DATOS

Existe la posibilidad de ceder a un tercero los datos personales siempre que sea para fines directamente relacionados con el propietario de los datos y el responsable del archivo, y siempre con el consentimiento previo del primero. Como siempre existen una serie de casos en el que no será necesario ese consentimiento:

- En el caso de ceder los datos a entes públicos de la Administración o de ámbito jurídico.
- Si se ceden los datos debido a una emergencia médica.
- Si la transferencia de los datos está autorizada por la ley.

Destacar, que cualquiera que reciba los datos deberá atenerse a las disposiciones de la LOPD que estamos tratando en este trabajo.

Se puede hablar de un caso especial, que es cuando los responsables de los datos se ven obligados a dar acceso a un tercero para que realice algún tipo de tratamiento con los datos del fichero. En este caso no se considera comunicación de datos pero deberá realizarse un contrato por escrito y cumplida la prestación de los servicios con los datos serán destruidos o devueltos al responsable.

## DERECHOS DE LAS PERSONAS

Será obligatorio que todo aquel encargado de recoger, tratar y ceder datos de carácter personal inscriba los ficheros, creados para el almacenamiento de estos datos, en el Registro General de la Agencia de Protección de Datos, haciendo figurar un responsable de fichero o tratamiento.

El tratamiento de datos de carácter personal puede permitir que se cree un perfil de la persona, es decir, saber cómo es, fuera de su control. Para evitar esto se conceden al ciudadano una serie de derechos (acceder, rectificar, cancelar aquellos datos que no sean exactos ) que le otorguen la facultad de poder ejercer un control sobre el uso de sus datos por parte de quienes los traten. Para ejercitar estos derechos es necesario el cumplimiento de unos requisitos formales, tales como el envío de una solicitud a dicho responsable (esta contendrá el nombre y apellidos del interesado o de su representante, fotocopia de su DNI, la petición en que se concreta la solicitud, etc.) sin gasto ninguno para el interesado. El responsable de tratamiento deberá contestar al interesado, tanto si es poseedor de sus datos como sino, y subsanar aquellos datos en caso de inexactitud. Los interesados podrán reclamar, de forma reglamentaria, ante la Agencia de Protección de Datos las actuaciones contrarias a lo dispuesto en la ley por parte del responsable del fichero.

A continuación se concretan los derechos que el interesado puede ejercitar ante el responsable del fichero respecto a los datos objeto de tratamiento.

## DERECHO DE CONSULTA AL REGISTRO GENERAL DE PROTECCIÓN DE DATOS

Con objeto de conocer la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento, para estar al tanto del uso de sus datos y controlar el perfil creado por estos, cualquier persona podrá consultar, pública y gratuitamente, el Registro General de Protección de Datos para obtener información a tal fin.

## DERECHO DE ACCESO

Derecho que podrá ejercitar cualquier interesado para solicitar y obtener información gratuita sobre que datos están siendo tratados, el origen de éstos y las cesiones o comunicaciones realizadas o que se prevén realizar. Cuando el interesado sea menor de edad o incapacitado se comprobará que el derecho se ejerce a través de un representante legal.

## DERECHOS DE RECTIFICACIÓN Y CANCELACIÓN

Otorgan la posibilidad al interesado de exigir al responsable del fichero que cumpla con el principio de calidad de datos, pudiendo solicitarle que rectifique aquellos datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la ley y, en particular, cuando éstos resulten inexactos o incompletos, y que los cancele cuando dejen de ser necesarios para el fin en el que hubieran sido registrados. Con esto se asegura que los datos se mantengan de forma adecuada y no excesiva en relación con el ámbito y finalidades legítimas para las que se recogieron. Los datos, totales o parciales, sobre los que se ejerciten los derechos de rectificación y cancelación podrán ser excluidos de un determinado fichero de datos personales, bien por ser erróneos o por negarse el titular a su tratamiento.

## DERECHO DE OPOSICIÓN

Supone que en los casos en los que no se requiera el consentimiento de éste para el tratamiento de sus datos, y siempre que una ley no disponga lo contrario, pueda oponerse al tratamiento de los mismos cuando existan motivos fundados y legítimos.

## DERECHO DE IMPUGNACIÓN DE VALORACIONES

Consiste en la facultad que se concede a las personas para no verse sometidas a las decisiones con efectos jurídicos basadas exclusivamente en un tratamiento de datos destinado a evaluar determinados aspectos de su personalidad o definición de sus características. El afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizado en el tratamiento que sirvió para adoptar dicha decisión.

## DISPOSICIONES SECTORIALES

Los ficheros de titularidad pública se rigen por un marco legal distinto al de los ficheros de titularidad privada, por este motivo el TÍTULO IV de LOPD se divide en dos capítulos que muestran la normativa para cada uno de estos dos tipos de ficheros.

## FICHEROS DE TITULARIDAD PÚBLICA

Regula el uso de los ficheros en la Administración Pública y en las Fuerzas y Cuerpos de Seguridad.

El Registro General de Protección de Datos (RGPD) es el órgano de la Agencia de Protección de Datos al que corresponde velar por la publicidad de la existencia de los ficheros de datos de carácter personal como veremos más adelante.

La **creación, modificación o supresión** de un fichero de titularidad pública solo podrá realizarse cuando aparezca publicado en el Boletín Oficial del Estado y deberá ser comunicado al Registro General de Protección de Datos detallando los siguientes puntos:

- Cual es su finalidad y para que se va a emplear.
  - Las personas a las que se las va a pedir sus datos y el procedimiento de recogida de estos.
  - La estructura que tendrá el fichero y los tipos de datos, así como la seguridad que deberán tener; básica, media o alta.
  - La Administración responsable del fichero. Como va a manipular los datos, o en su caso, la transferencia de estos a países terceros.
- En el caso de que se desee destruir un fichero deberá especificarse cual es el destino de los mismos y como serán destruidos.

Los ficheros realizados por una Administración **no serán comunicados a otras Administraciones** Públicas, salvo que, al ser creado el fichero, se haya establecido de ese modo o cuando sea para fines científicos, estadísticos o históricos. Queda excluida, bajo prevención de la ley, que los ficheros de titularidad pública se puedan transferir a alguno de carácter privado.

Todos los ficheros recogidos para fines administrativos (por parte de las **Fuerzas y Cuerpos de Seguridad**) estarán sujetos a la LOPD. Tan solo podrán recoger información sin el consentimiento de las personas afectadas cuando resulten necesarios para la prevención de un peligro real para la seguridad pública o para la prevención de infracciones penales.

Hay una serie de excepciones respecto al acceso del interesado a sus datos que se disponen en el título III cuando se trata de ficheros pertenecientes a las Administraciones. Los responsables de los cuerpos de seguridad podrán denegar el acceso al afectado cuando entienden que pone en peligro la seguridad pública o la defensa del estado y la Hacienda Pública también podrá negar el acceso o modificación de datos si se obstaculiza las actualizaciones destinadas a hacer cumplir las obligaciones tributarias.

## FICHEROS DE TITULARIDAD PRIVADA

Para poder inscribir un fichero privado en el RGPD se deberán dar los siguientes pasos:

- Notificación a la Agencia de Protección de Datos antes de su creación.
  
- Adjuntar los siguientes datos:
  - Responsable del fichero
  - Finalidad
  - Ubicación
  - Tipo de datos de carácter personal que contiene
  - Medidas de seguridad
  - Cesiones y transferencias que se prevean realizar
  
- Cualquier cambio se notificará a la Agencia de Protección de Datos
  
- Si después de un mes no hay noticias sobre la creación del fichero se considerará que éste ha sido inscrito en el RGPD

Datos de acceso público: El Censo promocional es un servicio que se brinda a quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia o actividades análogas. Este tipo de empresas podrán solicitar una copia del censo promocional con validez para un año. Este censo contendrá el nombre, apellidos y domicilio de los individuos que en él constan, pudiendo solicitar no aparecer en él.

Cualquier empresa dedicada a la publicidad y otras actividades análogas que usen datos de carácter personal deberán atenerse a los siguientes puntos:

- Los datos siempre serán de fuentes accesibles al público o facilitados por los propios interesados con su consentimiento.
  
- Los afectados tendrá derecho a conocer el origen de los datos así como el resto de información citada en apartados anteriores.
  
- Se debe brindar la posibilidad a los afectados de oponerse al tratamiento de sus datos.

Por último, comentar la existencia de Códigos Tipo, realizados mediante acuerdos entre empresas o convenios administrativos que establecen las condiciones de utilización de los ficheros de carácter personal en su entorno. En general, estos códigos tienen carácter deontológico o de buena práctica profesional y deberán ser depositados en el RGPD.

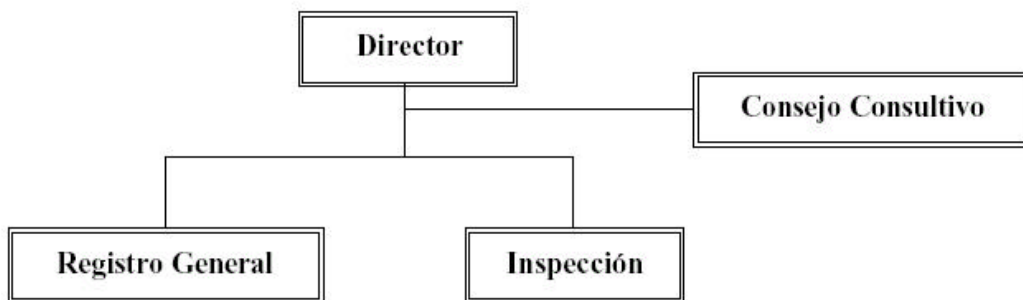
## MOVIMIENTO INTERNACIONAL DE DATOS

El trasiego de información de un país a otro (pensemos por ejemplo en el uso comercial de Internet) supone un traslado de grandes cantidades de datos de carácter personal, el cuál puede provocar perjuicios en la privacidad de las personas. Como norma general, la LOPD, establece que no se pueden efectuar transferencias de datos de carácter personal, que hayan o vayan a ser sometidos a tratamiento, a países que no proporcionen un nivel de protección equiparable al nuestro, salvo previa autorización del Director de la

Agencia de Protección de Datos. Como siempre existen una serie de excepciones en las que no será de aplicación la norma general: por ejemplo, cuando la transferencia resulte de la aplicación de tratados o convenios en los que sea parte España, cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional o cuando la transferencia sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios, esto entre los casos más importantes.

## AGENCIA DE PROTECCIÓN DE DATOS

La Agencia de Protección de Datos es la organización que vela por el cumplimiento de la LOPD. Su estructura es la siguiente:



- **DIRECTOR**: tiene consideración de alto cargo y será nombrado por el Consejo Consultivo. Tiene potestad para ejercer sus funciones de manera independiente y objetiva y, tan solo, deberá atender al Consejo Consultivo en la toma de decisiones.

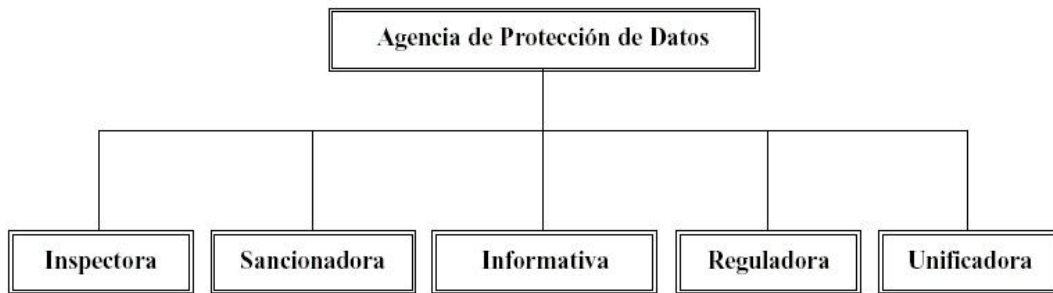
- **CONSEJO CONSULTIVO**: formado por:

- Un Diputado, Propuesto por el Congreso de los Diputados.
- Un Senador, propuesto por el Senado.
- Un representante de la Administración Central, propuesto por el Gobierno.
- Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias.
- Un miembro de la Real Academia de la Historia.
- Un experto en la materia, propuesto por el Consejo Superior de Universidades.
- Un representante de los usuarios y consumidores.
- Un representante de cada Comunidad Autónoma.
- Un representante del sector de ficheros privados.

- **REGISTRO GENERAL DE PROTECCIÓN DE DATOS**: órgano encargado del procedimiento de inscripción, modificación, cancelación, reclamación,... de los ficheros.

- **AUTORIDADES DE CONTROL**: encargadas de la inspección de los ficheros que trata esta ley.

Funciones de la Agencia de Protección de Datos:



- Velará por el cumplimiento de la legislación sobre protección de datos y controlará su aplicación.
- Sancionará y además atenderá las reclamaciones realizadas por personas afectadas.
- Informará a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.
- Emitirá las autorizaciones previstas en la Ley y dictará las instrucciones precisas para adecuar los tratamientos a los principios de la LOPD.
- Desempeñará las funciones necesarias para el movimiento internacional de los datos realizando una labor unificadora en el ámbito internacional.

Además algunas de las responsabilidades de la Agencia de Protección de Datos estarán delegadas en los órganos correspondientes de las Comunidades Autónomas.

De cualquier modo, el director de la Agencia de Protección de Datos tiene la última palabra en la aplicación de la LOPD por encima de todos los restantes miembros.

### INFRACCIONES Y SANCIONES

La LOPD establece un régimen sancionador al que se encuentran sujetos tanto los responsables de los ficheros como los encargados de los tratamientos. Este régimen fija tres niveles de infracción, clasificados en leves, graves y muy graves, los cuales llevan asociadas la imposición de las correspondientes sanciones económicas.

#### TIPOS DE INFRACCIONES:

##### - LEVES:

- No atender la solicitud del interesado de rectificación o cancelación de los datos sujetos a tratamiento cuando proceda legalmente.
- No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.
- No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

- Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la LOPD.
  - Incumplir el deber de secreto establecido en el artículo 10 de la LOPD, salvo que constituya infracción grave.
- GRAVES:
- Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general.
  - Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.
  - Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos de que éste sea exigible.
  - Tratar los datos de carácter personal o usarlos posteriormente infringiendo los principios y garantías establecidos en la LOPD o con el incumplimiento de los mandatos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituye infracción muy grave.
  - El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.
  - Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la LOPD ampara.
  - La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.
  - Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.
  - No remitir a la Agencia de Protección de Datos las notificaciones previstas en la LOPD o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.
  - La obstrucción al ejercicio de la función inspectora.

- No inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.
  - Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de la LOPD, cuando los datos hayan sido recabados de persona distinta del afectado.
- MUY GRAVES:
- La recogida de datos en forma engañosa y fraudulenta.
  - La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.
  - Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.
  - No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.
  - La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.
  - Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.
  - La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7 (ver anexo I), así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.
  - No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
  - No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

#### TIPOS DE SANCIONES:

Leves: 600 a 60000 € Prescriben al año.

Graves: 60000 a 300000 € Prescriben a los dos años.

Muy Graves: 300000 a 600000 € Prescriben a los tres años.

Cuando cualquiera de las infracciones de estos tres niveles se cometan en ficheros cuyos responsables son las Administraciones públicas, el Director de la Agencia de Protección de Datos tomará las medidas oportunas para que cesen o se corrijan los efectos de la infracción, notificándolo al responsable del fichero, al órgano del que depende y a los afectados. Las sanciones aplicadas en este caso, serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas.

## REGLAMENTO DE MEDIDAS DE SEGURIDAD

Sin duda, este es uno de los temas que más interesan desde el punto de vista del afectado para saber cuales son los métodos de seguridad que se utilizan para proteger sus datos de carácter personal.

El objeto de este reglamento es el desarrollo de lo dispuesto en la LORTAD referente a la seguridad de los ficheros automatizados, centros de tratamiento y locales, equipos, sistemas y programas, y personas que intervengan en el tratamiento de los datos, y mientras no se oponga a las directivas de la LOPD no estará sujeto a modificaciones.

Con este reglamento se pretende asegurar la confidencialidad e integridad de la información, la intimidad personal y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado.

## NIVELES DE SEGURIDAD

Dependiendo de la naturaleza de la información y del grado de necesidad de garantizar su confidencialidad e integridad, las medidas de seguridad se pueden clasificar en tres niveles, que son: básico, medio y alto. Estas medidas pueden ser técnicas u organizativas, pudiendo ser las técnicas de tipo físico o lógico.

### **NIVEL BASICO:**

Con este nivel de seguridad se tratan:

- Todos los ficheros que contengan datos de carácter personal.

El **documento de seguridad** es un documento elaborado por el responsable del fichero que contiene la normativa de seguridad, cuyo cumplimiento es obligatorio para todo el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información. Su contenido se centra básicamente en:

- Ámbito de aplicación (por ejemplo, bases de datos en donde se encuentra la información)
- Política de seguridad
- Funciones y obligaciones del persona
- Estructura de los ficheros y descripción de los sistemas de información que los tratan
- Procedimientos de notificación, gestión y respuesta a las incidencias

- Procedimientos de realización de copias de respaldo

El responsable del fichero dará a conocer al personal con acceso a los datos y al sistema de información las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias de su incumplimiento.

El responsable del fichero se encarga de que exista una relación actualizada de usuarios con acceso autorizado al sistema de información y de implantar procedimientos de identificación y autenticación para dicho acceso. En la relación de usuarios se reflejan los derechos de acceso autorizados para cada uno de ellos (lectura, acceso parcial a datos, etc.).

El mecanismo de autenticación puede basarse en la existencia de contraseñas, en cuyo caso habrá un procedimiento de asignación, distribución y almacenamiento ininteligible que garantice su confidencialidad e integridad. Estas se cambiarán de forma periódica según determine el documento de seguridad.

Entre las medidas de seguridad de tipo físico destacan:

Los soportes informáticos que contengan datos de carácter personal (disquetes, cintas, etc.) deberán estar inventariados e identificados de forma expresa y estarán almacenados en un lugar restringido al personal autorizado.

Realización de copias de respaldo y definir una correcta aplicación de los procedimientos de recuperación de los datos mediante estas copias.

## **NIVEL MEDIO:**

Se mantendrán en este nivel de seguridad los ficheros que contengan datos relativos a

- Comisión de infracciones administrativas o penales.
- Hacienda pública.
- Servicios financieros.
- Solvencia patrimonial y crédito.

Además de las medidas de seguridad del nivel básico, este nivel se ampliará con lo siguiente.

En el documento de seguridad, además de lo contenido en el nivel básico se incluirá la identificación del responsable o responsables de seguridad, los controles periódicos a realizar para verificar el cumplimiento del documento y las medidas que se van a adoptar cuando un fichero vaya a ser desechado o reutilizado.

El responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas establecidas en el documento de seguridad. Esto no supone la delegación de la responsabilidad que corresponde al responsable del fichero.

Al menos cada dos años, y como medida de seguridad organizativa, los sistemas de información e instalaciones de tratamiento de datos se verán sometidos a una auditoría, interna o externa, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, con el fin de verificar el cumplimiento del reglamento. El informe de la auditoría quedará a disposición de la Agencia de Protección de Datos.

A la hora de intentar acceder al sistema de información se limitará el número de intentos de acceso no autorizados.

Sólo el personal autorizado (el indicado en el documento de seguridad) tendrá acceso a los locales dónde se encuentren los sistemas de información con datos de carácter personal.

Se establecerán sistemas de registro de entrada y salida de soportes informáticos que permitan, directa o indirectamente, conocer:

- El tipo de soporte.
- La fecha y la hora.
- El emisor y el destinatario, respectivamente.
- El número de soportes.
- El tipo de información que contienen.
- La forma de envío.
- La persona autorizada responsable de la recepción y entrega, respectivamente.

En definitiva se trata de realizar un inventario de soportes.

En el registro de incidencias constarán los procedimientos realizados para la recuperación de datos de un fichero desechado.

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

## **NIVEL ALTO:**

Se intentará proteger mediante este nivel a los ficheros que contengan datos sobre

- Ideología.
- Religión.
- Creencias.
- Origen racial.
- Salud.
- Vida sexual.
- Y recabados para fines policiales sin consentimiento de las personas afectadas.

Este nivel estará compuesto por las medidas de seguridad del nivel básico, más las correspondientes al nivel medio, más las de tipo lógico y físico que se citan a continuación.

La distribución de soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

Se mantendrá un registro de acceso a los ficheros en donde por cada acceso se guardará básicamente:

- La identificación del usuario.
- La fecha y la hora en que se realizó.
- El fichero accedido.
- El tipo de acceso.
- Si ha sido autorizado o denegado.

Todos estos datos se mantendrán durante, al menos, dos años.

Además de lo dispuesto para el nivel básico, se deberá conservar una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se efectúa el tratamiento de éstos. Por tanto, las copias de seguridad no pueden estar en el mismo local que los ordenadores.

La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

## DIFERENCIAS ENTRE LA LORTAD Y LOPD

### ¿PORQUÉ UNA NUEVA LEY Y NO UNA MODIFICACIÓN DE LA LORTAD DE 1992?

La tramitación parlamentaria de la nueva Ley ha sido una especie de técnica jurídica más que cuestionable. Sus orígenes se encuentran en agosto de 1998 momento en el que el Gobierno remitió al Parlamento un Proyecto de Ley de modificación de la LORTAD en el que, tras reconocerse que la LORTAD se ajustaba en gran medida a los mandatos de la Directiva 95/46/EC, se proponían (en tres páginas) algunas modificaciones.

Sin embargo, ante las 114 enmiendas presentadas al Proyecto inicial, los diputados encargados de redactar el Informe sobre el Proyecto de Ley decidieron proponer un texto nuevo completo derogando la Ley anterior. Tras una larga y controvertida tramitación parlamentaria, el Congreso de los Diputados aprobó a finales de noviembre de 1999 el texto de la nueva Ley.

La nueva Ley carece de Exposición de Motivos que explique qué motivos han llevado a su aprobación cuando la LORTAD había sido aprobada tan sólo siete años antes.

Ni siquiera se preocupa en mencionar la Directiva 95/46/EC (como exige su art. 32.1). Y es que la razón de ser de la nueva Ley no es, desde luego, la transposición de los mandatos de la Directiva.

La nueva Ley refleja el trauma que supuso la aplicación de la LORTAD de 1992 y el intento, lamentablemente fallido, de solucionar todos los problemas que dicha Ley ocasionó. En este sentido, la nueva Ley es fruto del lobby de todos los sectores empresariales afectados por la Ley de 1992 (empresas de marketing, credit bureau, entidades financieras y aseguradoras), de las peculiaridades que implica el modelo español de Estado de Comunidades Autónomas y, por último, de los acuerdos parlamentarios que precisaba un Gobierno que, en aquel entonces, no tenía mayoría en las Cámaras legislativas para aprobar esta Ley.

Lamentablemente, analizando el contenido de la nueva Ley no creemos que se vayan a superar los problemas que supuso la Ley de 1992. Pero, pasemos, sin más dilación, a señalar aquellos aspectos de la nueva Ley que de mayor interés resultarán a los lectores.

---

La LORTAD fue la precursora de la actual LOPD, pero desde su aceptación ha sido perseguida por la polémica y el desacuerdo. Para entender mejor la nueva ley que la sustituye es importante hacer una comparación entre ambas e intentar encontrar los puntos que difieren para poder observar la evolución que ha sufrido el tratamiento de datos de carácter personal desde 1992 hasta la actualidad en el ámbito jurídico español.

Las diferencias comienzan ya en el nombre. La eliminación de una palabra en el objeto de la nueva ley: "automatizados", tiene una enorme trascendencia a la hora de analizar ambas leyes. Se ha cambiado el fin último de la LORTAD y sin embargo permanece vigente gran parte de su articulado.

La LORTAD, según se expone, de una forma que no deja lugar a ninguna duda, en su artículo primero tenía por objeto el desarrollo del artículo 18.4 de la Constitución.

En la LORTAD no tenían en cuenta otro tipo de datos que los de carácter personal y siempre que fuesen tratados de forma automatizada, la posesión de este tipo de datos, pero en otro soporte, no era objeto de la misma. Se establecía, por decirlo así, una categoría de datos: los automatizados, algo que en la LOPD ha dejado de existir.

La LORTAD se refería sólo a los datos organizados automatizados aunque posponía para fecha posterior, a juicio del Gobierno, la posible incorporación al ámbito de la Ley los no automatizados.

La desaparición de esa distinción de automatizados englobando a todos los datos de carácter personal en una misma categoría cambia el panorama y en la práctica plantea la necesidad de estudiar la nueva situación creada.

El objeto de la LOPD pretende ser mucho más amplio que el de la LORTAD, en esta finalidad estaba clara y era muy específica: cumplir el mandato constitucional de desarrollar el artículo 18.4 de la Constitución para limitar el uso de algo que se consideraba pernicioso. En el caso de la LOPD ya no se trata de un artículo sino de la sección 1ª de la Constitución: “De los derechos fundamentales y las libertades públicas.”

### ÁMBITO DE APLICACIÓN

El ámbito de aplicación de la LOPD se mueve en torno a tres parámetros: de contenido, territorial y temporal.

Entran dentro de su ámbito todos los tratamientos de datos automatizados o no de carácter personal concernientes a personas físicas. En el aspecto territorial abarca a los ficheros no sólo cuando el responsable del tratamiento esté establecido en territorio español sino cuando no lo está pero utiliza medios situados en el mismo o le sean de aplicación las normas internacionales.

Por último, en principio, la temporalidad le viene impuesta por la necesidad de disponer de los datos para el fin para el que se creó el fichero o bien para una finalidad posterior no compatible con aquella.

La LOPD, siendo consecuente con la filosofía seguida por la LORTAD de que haya siempre un responsable cuando hay que hacer frente al daño producido por una posible infracción, establece que la ley alcanza al responsable del tratamiento aunque no resida en territorio español y obliga a que cuando el responsable del tratamiento no está establecido en territorio de la U.E. deba designar un representante en España.

Conocer en la antigua ley si un tipo de registro era una fuente accesible al público algunas veces no era tarea fácil.

La LORTAD definía las fuentes accesibles al público como aquellos ficheros automatizados de titularidad pública cuyo objeto legalmente establecido fuese el almacenamiento de datos para su publicidad con carácter general.

En la LOPD se consideran fuentes accesibles al público las siguientes:

- Censo promocional.
- Repertorios telefónicos (normativa específica).
- Listas de personas pertenecientes a grupos profesionales.
- Diarios oficiales.
- Boletines oficiales.
- Medios de comunicación.

De esta forma las dudas que se planteaban sobre si un fichero determinado contenía o no datos accesibles al público ahora con la nueva normativa no se presentan.

### LOS PRINCIPIOS DE LA LEY

No se han producido muchas modificaciones en los principios que inspiran la Ley.

En el artículo 4 punto 2 se produce en la LOPD el cambio de una palabra que puede tener gran importancia a la hora de la aplicación práctica de la Ley.

La LORTAD decía: “no podrán usarse para finalidades distintas”, sin embargo la LOPD no habla de finalidades distintas sino incompatibles.

Con la nueva redacción muchas organizaciones que poseen grandes bases de datos y cuya finalidad en el momento de la recogida de los datos era simplemente, por ejemplo, la facturación de un servicio, ahora podrán utilizarlas para otros fines distintos de éste siempre que no sean incompatibles con el mismo algo que hasta ahora legalmente no podían hacer.

El artículo 9 relativo a la seguridad de los datos no sufre prácticamente transformación alguna; sin embargo su desarrollo reglamentario sí que las debe sufrir, ya que el reglamento, que también se trata en este trabajo, fue desarrollado para regular ficheros automatizados y a ellos va dirigido todo su articulado por lo que el cambio que hay que realizar tiene que ser sustancioso. Probablemente se presentarán problemas a la hora de adaptar dicho reglamento.

A la prestación de servicios por un tercero, el outsourcing, la LOPD le dedica mayor atención incluyéndola bajo el epígrafe: “Acceso a los datos por cuenta de terceros” en el artículo 12 que figura en el Título referido a los principios de la protección de datos.

Una vez cumplida la prestación de servicios los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto del tratamiento.

La LORTAD le dedicaba el artículo 27 dentro de los ficheros de titularidad privada y se limitaba a cinco años el tiempo en que el prestador del servicio podía almacenar los datos mediante autorización del responsable del fichero.

La LOPD no especifica tiempo alguno por lo que se presume que podrán almacenarse en tanto sean necesarios para la prestación periódica del servicio.

## DERECHOS DE LAS PERSONAS

Los derechos de las personas que se configuran en la LOPD son: impugnación de valoraciones, consulta, acceso, rectificación y cancelación, oposición, tutela e indemnización.

El derecho de impugnación de valoraciones que en la LORTAD se refería a las producidas por un tratamiento automatizado, en la LOPD es más general refiriéndose a cualquier tipo de tratamiento.

El derecho de acceso se regula como un derecho gratuito, cosa que no se hacía en la LORTAD y entre la información que se tiene que facilitar aparte de los datos de carácter personal y el origen de los mismos se debe informar de las cesiones realizadas y de las que se tenga previsto realizar.

En los derechos de rectificación y cancelación se introduce en el artículo el plazo de diez días para hacer efectivos los mismos, que es superior al plazo de cinco días que establecía la LORTAD.

El derecho de oposición se configura como el derecho que tienen los interesados, en determinadas circunstancias, a oponerse al tratamiento de los datos que les conciernen, en cuyo caso, previa petición y de forma gratuita serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren.

## OTRAS DIFERENCIAS

Con la LOPD nace el llamado Censo Promocional, se trata de una copia de datos de:

nombre, apellidos y domicilio que constan en el censo electoral. Este se podrá usar durante un año para fines publicitarios.

En los artículos correspondientes al movimiento internacional de datos se enumeran las circunstancias que debe evaluar la Agencia de Protección de Datos para que el nivel de protección que ofrece el país se considere adecuado, asimismo se amplían las excepciones a la Ley en esta área, siguiendo la Directiva comunitaria.

Los tipos de infracciones siguen dividiéndose en leves, graves y muy graves habiéndose modificado en algunos aspectos.

El carácter de muy grave se reserva para los datos especialmente protegidos y los recabados con fines policiales.

Se incluyen entre los graves algunos casos mas como: no inscribir el fichero cuando haya sido requerido para ello e incumplir el deber de información cuando los datos se recaben de persona distinta del afectado.

Las infracciones muy graves también han visto incrementados sus casos: no atender u obstaculizar de forma sistemática el ejercicio de los derechos de los interesados y no atender de igual forma la notificación de inclusión en un fichero.

## LEYES DE PROTECCIÓN DE DATOS EN OTROS PAISES

### **ALEMANIA**

En Alemania, para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos:

- Espionaje de datos.
- Estafa informática .
- Falsificación de datos probatorios. junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos.
- Alteración de datos es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.
- Sabotaje informático.
- Destrucción de datos de especial significado por medio de deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- Utilización abusiva de cheques o tarjetas de crédito.
- Por lo que se refiere a la estafa informática, el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos o a través de una intervención ilícita. Esta solución fue también adoptada en los Países Escandinavos y en Austria.

### **AUSTRIA**

Según la Ley de reforma del Código Penal del 22 de diciembre de 1987, se contemplan los siguientes delitos:

- Destrucción de datos (art. 126) no solo datos personales sino también los no personales y los programas.
- Estafa informática (art. 148) se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

### **CHILE**

Chile fue el primer país latinoamericano en sancionar una Ley contra Delitos Informáticos. La ley 19223 publicada en el Diario Oficial (equivalente del Boletín Oficial argentino) el 7 de junio de 1993 señala que la destrucción o inutilización de un sistema de tratamiento de información puede ser castigado con prisión de un año y medio a cinco.

Como no se estipula la condición de acceder a ese sistema, puede encuadrarse a los autores de virus. Si esa acción afectara los datos contenidos en el sistema, la prisión se establecería entre los tres y los cinco años.

El hacking, definido como el ingreso en un sistema o su interferencia con el ánimo de apoderarse, usar o conocer de manera indebida la información contenida en éste, también es pasible de condenas de hasta cinco años de cárcel; pero ingresar en ese mismo sistema sin permiso y sin intenciones de ver su contenido no constituye delito.

Dar a conocer la información almacenada en un sistema puede ser castigado con prisión de hasta tres años, pero si el que lo hace es el responsable de dicho sistema puede aumentar a cinco años. Esta ley es muy similar a la inglesa aunque agrega la protección a la información privada.

## **CHINA**

El Tribunal Supremo Chino castigará con la pena de muerte el espionaje desde Internet, según se anunció el 23 de enero de 2001. Todas las personas "implicadas en actividades de espionaje", es decir que "roben, descubran, compren o divulguen de secretos de Estado" desde la red podrán ser condenada a penas que van de diez años de prisión hasta la muerte.

La corte determina que hay tres tipos de actividades donde la vigilancia será extrema: secretos de alta seguridad, los secretos estatales y aquella información que dañe seriamente la seguridad estatal y sus intereses. El comité permanente de la Asamblea Nacional Popular (ANP) estableció una lista de actividades ilegales, tales como la infiltración de documentos relacionados con el Estado, la defensa o las tecnologías punta, o la difusión de virus informático.

El Tribunal ha hecho especial énfasis al apartado del espionaje desde la red. A los llamados "criminales", además de tener asegurada una severa condena (la muerte), también se les puede confiscar los bienes.

## **ESTADO UNIDOS DE AMÉRICA**

El primer abuso de una computadora se registró en 1958 mientras que recién en 1966 se llevó adelante el primer proceso por la alteración de datos de un banco de Mineapolis. En la primera mitad de la década del 70, mientras los especialistas y criminólogos discutían si el delito informático era el resultado de una nueva tecnología o un tema específico, las ataques computacionales se hicieron más frecuentes. Para acelerar las comunicaciones, enlazar compañías, centros de investigación y transferir datos, las redes debían (y deben) ser accesibles, por eso el Pentágono, la OTAN, las universidades, la NASA, los laboratorios industriales y militares se convirtieron en el blanco de los intrusos.

Pero en 1976 dos hechos marcaron un punto de inflexión en el tratamiento policial de los casos: el FBI dictó un curso de entrenamiento para sus agentes acerca de delitos informáticos y el Comité de Asuntos del Gobierno de la Cámara presentó dos informes que dieron lugar a la Ley Federal de Protección de Sistemas de 1985 Esta ley fue la base para que Florida, Michigan, Colorado, Rhode Island y Arizona se constituyeran en los primeros estados con legislación específica, anticipándose un año al dictado de la Computer Fraud y Abuse Act de 1986.

El acta se refiere en su mayor parte a delitos de abuso o fraude contra casas financieras, registros médicos, computadoras de instituciones financieras o involucradas en delitos interestatales. También especifica penas para el tráfico de claves con intención de

cometer fraude y declara ilegal el uso de passwords ajenas o propias en forma inadecuada. Pero sólo es aplicable en casos en los que se verifiquen daños cuyo valor supere el mínimo de mil dólares.

Se contempla la regulación de los virus (computer contaminant) conceptualizándolos aunque no los limita a los comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos. Modificar, destruir, copiarlos, transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas es considerado delito.

El aumento en la cantidad de casos de hacking y la sensación de inseguridad permanente que generaron (fomentada por la difusión de los hechos en programas especiales de televisión y artículos de revistas especializadas), cambiaron la percepción de las autoridades con respecto a los hackers y sus ataques. Los casos que demostraron ese cambio fueron los del "Condor" Kevin Mitnick y los de "ShadowHawk" Herbert Zinn hijo.

El FCIC (Federal Computers Investigation Committee), es la organización más importante e influyente en lo referente a delitos computacionales: los investigadores estatales y locales, los agentes federales, abogados, auditores financieros, programadores de seguridad y policías de la calle trabajan allí comunitariamente. El FCIC es la entrenadora del resto de las fuerzas policiales en cuanto a delitos informáticos, y el primer organismo establecido en el nivel nacional.

Además existe la Asociación Internacional de Especialistas en Investigación Computacional (IACIS), quien investiga nuevas técnicas para dividir un sistema en sus partes sin destruir las evidencias. Sus integrantes son "forenses de las computadoras" y trabajan, además de los Estados Unidos, en el Canadá, Taiwán e Irlanda.

## **FRANCIA**

La Ley 88/19 del 5 de enero de 1988 sobre el fraude informático contempla:

- Acceso fraudulento a un sistema de elaboración de datos. Se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.
- Sabotaje Informático. Falsear el funcionamiento de un sistema de tratamiento automático de datos.
- Destrucción de datos. Se sanciona a quien intencionalmente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos, suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.
- Falsificación de documentos informatizados. Se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

## **HOLANDA**

Hasta el día 1 de marzo de 1993 Holanda era un paraíso para los hackers.

Pero ese día entró en vigencia la Ley de Delitos Informáticos, con artículos específicos sobre técnicas de hacking.

El mero hecho de entrar en una computadora en la cual no se tiene acceso legal ya es delito y puede ser castigado hasta con seis meses de cárcel. Si se usó esa computadora

hackeada para acceder a otra, la pena máxima sube a cuatro años aunque el crimen, a simple vista, no parece ser peor que el anterior. Copiar archivos de la máquina hackeada o procesar datos en ella también conlleva un castigo de cuatro años en la cárcel. Publicar la información obtenida es ilegal si son datos que debían permanecer en secreto, pero si son de interés público es legal. El daño a la información o a un sistema de comunicaciones puede ser castigado con cárcel de seis meses a quince años, aunque el máximo está reservado para quienes causaron la muerte de alguien con su accionar. Cambiar, agregar o borrar datos puede ser penalizado hasta con dos años de prisión pero, si se hizo vía remota aumenta a cuatro.

Los virus están considerados de manera especial en la ley. Si se distribuyen con la intención de causar problemas, el castigo puede llegar hasta los cuatro años de cárcel; si simplemente se "escapó", la pena no superará el mes.

El usar el servicio telefónico mediante un truco técnico (Phreaking) o pasando señales falsas con el objetivo de no pagarlo puede recibir hasta tres años de prisión. La venta de elementos que permitan el phreaking se castiga con un año de prisión como tope y si ese comercio es el modo de ganarse la vida del infractor, el máximo aumenta a tres. La ingeniería social también es castigada con hasta tres años de cárcel. Recibir datos del aire es legal (transmisiones satelitales), siempre y cuando no haga falta un esfuerzo especial para conseguirlos; la declaración protege datos encriptados, como los de ciertos canales de televisión satelital. Falsificar tarjetas de crédito de banca electrónica y usarlas para obtener beneficios o como si fueran las originales está penado con hasta seis años. Aunque hacerlas y no usarlas parece es legal.

## **INGLATERRA**

Luego de varios casos de hacking surgieron nuevas leyes sobre delitos informáticos. En agosto de 1990 comenzó a regir la Computer Misuse Act (Ley de Abusos Informáticos) por la cual cualquier intento, exitoso o no de alterar datos informáticos con intención criminal se castiga con hasta cinco años de cárcel o multas sin límite.

El acceso ilegal a una computadora contempla hasta seis meses de prisión o multa de hasta dos mil libras esterlinas. El acta se puede considerar dividida en tres partes: hackear (ingresar sin permiso en una computadora), hacer algo con la computadora hackeada y realizar alguna modificación no autorizada.

El último apartado se refiere tanto al hacking (por ejemplo, la modificación de un programa para instalar un backdoor), la infección con virus o, yendo al extremo, a la destrucción de datos como la inhabilitación del funcionamiento de la computadora.

Bajo esta ley liberar un virus es delito y en enero de 1993 hubo un raid contra el grupo de creadores de virus. Se produjeron varios arrestos en la que fue considerada la primera prueba de la nueva ley en un entorno real.

A continuación se exponen el concepto de fraude informático así como algunos casos reales, en los que de alguna manera se ha cometido fraude, infringiendo alguna de las leyes jurídicas, basadas en la prevención de delitos informáticos:

## **DELITOS INFORMÁTICOS**

### **CONCEPTO DE FRAUDE INFORMÁTICO**

#### **Fraude Informático**

"Con el avance de las nuevas tecnologías, la informática se ha convertido en un instrumento que nos proporciona infinitas posibilidades de desarrollo y progreso. Sin embargo, se ha dado lugar a una nueva forma de delincuencia, la delincuencia informática, ya que esta tecnología pone a disposición del delincuente un abanico de nuevas técnicas y métodos para alcanzar sus propósitos criminales" . El fraude informático es uno de los fenómenos más importante dentro de la delincuencia informática, dado al creciente aumento de las manipulaciones fraudulentas, y es por tanto la zona más inexplorada y la que mayores problemas enfrente en cuanto a su prevención, detección y represión.

Debe señalarse, a este respecto, que con la incursión de la informática en el sistema financiero, se ha reemplazado muchos de los documentos tradicionales en soporte papel, en los que constan las operaciones y saldos de cada uno de los clientes, por "anotaciones en cuenta" o registros lógicos realizadas en los sistemas informáticos, sin un soporte en papel o con reflejos en papel meramente informativos o secundarios. De ahí que la doctrina haya centrado el estudio del problema desde el enfoque de las manipulaciones de datos informatizados.

Asimismo, se ha sostenido que estas manipulaciones constituyen la forma más frecuente de comisión de delitos por medios informáticos, máxime ser una de las zonas de más temprana aparición.

Cuando se tuvo noticias de los primeros casos de fraude informático, éstos fueron vinculados al delito de estafa. Así se trato de encajar esta nueva figura dentro de los moldes estrechos de dicho tipo clásico, lo que a la postre supuso una dificultad para su encuadre, ya que los mismos elementos que configuraban a la estafa no lo permitían. Es así como nacieron entonces en la doctrina extranjera las discusiones acerca de la imposibilidad de engañar a una máquina, o de la existencia de un error psicológico por parte del computador que lo lleva a la disposición patrimonial lesiva .

Por tales razones y al verse el tipo penal de la estafa desbordado por los nuevos avances tecnológicos aplicados por los delincuentes para efectuar sus defraudaciones, llevaron a que naciera un nuevo tipo delictivo, el fraude informático, que vendría a absorber todas aquellas conductas defraudatorias que, por tener incorporada la informática como herramienta de comisión, no podían ser subsumidas en el tipo clásico de la estafa.

En nuestro país la vocación del tipo penal de estafa (Art. 563 del Código Penal), para incluir en su estructura constitutiva, los supuestos y conductas que entrañan al fraude informático, es prácticamente insuficiente, dado a que su propia estructura constitutiva seria el obstáculo para que dichos supuestos y conductas pudieran ser subsumidos en dicho tipo clásico.

Esta vinculación con la estafa desde sus inicios determinó además que el concepto, estructura y contenido del fraude informático fueran contruidos a partir de los elementos del delito de estafa.

#### 1.1. Concepto de Fraude Informático

E fraude informático, es "la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o ya contenidos en el ordenador en cualquiera de las fases de su procesamiento o tratamiento informático, con ánimo de lucro y en perjuicio de un tercero" .

Hace referencia tanto a las manipulaciones de entrada de datos (fase Input) como a las manipulaciones de salida (fase Output). Cabe mencionar que se debe tomar en cuenta que dichas manipulaciones también pueden ser realizadas en forma distinta, por ejemplo, a distancia y en cajeros bancarios automáticos.

Lo que importa aquí es que la acción del sujeto activo vaya encaminada a la modificación de el resultado de un procesamiento automatizado de datos, para así lograr un enriquecimiento injusto en detrimento del patrimonio de un tercero, hay una apropiación ilícita de dinero, bienes o servicios ajenos.

Para poder llegar a un concepto sobre el fraude informático, fijar nuestra atención en dos datos claves que son básicos para entender este fenómeno que es tanto la noción de fraude como de lo informático.

#### A. Noción de Fraude y Defraudación.

La defraudación ES EL PERJUICIO ECONÓMICO OCASIONADO MEDIANTE FRAUDE, EL CUAL COMPRENDE NO SÓLO EL ENGAÑO Y EL ABUSO DE CONFIANZA SINO TAMBIÉN EL USO DE OTROS MEDIOS FRAUDULENTOS, QUE NO SOLO AFECTAN EL PATRIMONIO INDIVIDUAL DE UNA PERSONA, SINO QUE TAMBIÉN LESIONAN OTROS INTERESES ECONÓMICOS DE CARÁCTER MACROSOCIAL .

#### B. En cuanto al carácter "Informático" del Fraude.

El fraude informático será: "EL CONJUNTO DE CONDUCTAS MALICIOSAS, QUE VALIÉNDOSE DE CUALQUIER MANIPULACIÓN FRAUDULENTA, MODIFIQUEN O INTERFIERAN EL FUNCIONAMIENTO DE UN PROGRAMA INFORMÁTICO, SISTEMA INFORMÁTICO, SISTEMA TELEMÁTICO O ALGUNA DE SUS PARTES COMPONENTES, PARA PRODUCIR UN PERJUICIO ECONÓMICO DE CUALQUIER ÍNDOLE" .

### ¿QUIÉN COMETE ESTAFA?

CODIGO PENAL. TITULO XIII. CAPITULO VI. DE LAS DEFRAUDACIONES

## SECCION 1.ª DE LAS ESTAFAS

### Artículo 248.

Se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigán la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

### Artículo 249.

Los reos de estafa serán castigados con la pena de prisión de seis meses a cuatro años, si la cuantía de lo defraudado excediere de cincuenta mil pesetas. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre éste y el defraudador, la medios empleados por éste y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción.

### Artículo 250.

1. El delito de estafa será castigado con las penas de prisión de uno a seis años y multa de seis a doce meses, cuando:

1.º Reaiga sobre cosas de primera necesidad, viviendas u otros bienes de reconocida utilidad social.

2.º Se realice con simulación de pleito o empleo de otro fraude procesal.

3.º Se realice mediante cheque, pagaré, letra de cambio en blanco o negocio cambiario ficticio.

4.º Se perpetre abusando de firma de otro, o sustrayendo, ocultando o inutilizando, en todo o en parte, algún proceso, expediente, protocolo o documento público u oficial de cualquier clase.

5.º Reaiga sobre bienes que integren el patrimonio artístico, histórico, cultural o científico.

6.º Revista especial gravedad, atendiendo al valor de la defraudación, a la entidad del perjuicio y a la situación económica en que deje a la víctima o a su familia.

7.º Se cometa abuso de las relaciones personales existentes entre víctima y defraudador, o aproveche éste su credibilidad empresarial o profesional.

2. Si concurrieran las circunstancias 6.ª o 7.ª con la 1.ª del número anterior, se impondrán las penas de prisión de cuatro a ocho años y multa de doce a veinticuatro meses.

### Artículo 251.

Será castigado con la pena de prisión de uno a cuatro años:

1.º Quien, atribuyéndose falsamente sobre una cosa mueble o inmueble facultad de disposición de la que carece, bien por no haberla tenido nunca, bien por haberla ya ejercitado, la enajenare, gravare o arrendare a otro, en perjuicio de éste o de tercero.

2.º El que dispusiere de una cosa mueble o inmueble ocultando la existencia de cualquier carga sobre la misma, o el que, habiéndola enajenado como libre, la gravare o enajenare nuevamente antes de la definitiva transmisión al adquirente, en perjuicio de éste, o de un tercero.

3.º El que otorgare en perjuicio de otro un contrato simulado.

### **Casos reales de estafas informáticas:**

#### **CASO DE TARJETAS DE CRÉDITO**

Hace un tiempo, fueron detenidos en Buenos Aires, 19 jóvenes que consiguieron los números y claves de tarjetas de crédito a través de la Red e hicieron numerosas compras con cargo a las mismas. Realizaban sus compras virtuales a "Amazon" y a "CD Now", y eran cargadas a dichas tarjetas de crédito, por lo que sus propietarios denunciaron la situación a "Argencard", que era la empresa responsable de la gestión de las mismas, la cual lo puso en conocimiento de las autoridades. Esta figura es conocida como Carding.

#### **ESTAFAS E INTERNET**

Internet se ha convertido en un medio muy susceptible a la comisión de estafas, debido a la escasa seguridad que todavía aporta la Red y a la pericia de muchos sujetos entendidos en el tema y que no dudan de aprovechar sus conocimientos en beneficio propio perjudicando a terceros.

Otra estafa se produce cuando en un sitio de contenido para adultos se ofrecen visualizar las imágenes gratis tras descargar un programa necesario para ello. Este es el caso del sitio sexygirls.com, cuyos usuarios se descargaron un visor de imágenes que en realidad era un Caballo de Troya, que silenciaba el módem del usuario y lo desconectaba de su proveedor de acceso a Internet y lo conectaba a un número de teléfono de Moldavia (antigua Unión Soviética), desde donde se redirigía la llamada a Norteamérica, donde se encontraban las imágenes solicitadas por el internauta. La factura telefónica alcanzaba cifras astronómicas ya que, aunque el sujeto abandonara el sitio, continuaba conectado a Moldavia.

## COMPRAS POR INTERNET

Gracias a un portal de Internet de los muchos que hay, se vió que era relativamente fácil conseguir puntos (similares a esos que se ganan en un concurso de la televisión) los cuales valían luego para comprar en una tienda virtual.

La manera de canjear estos puntos por descuentos era que te ofrecían un bono (un número de varios dígitos generado por algún algoritmo) y que luego, introducido a la hora de realizar la compra descontaba la cantidad elegida.

Pues bien, estos bonos, eran de un solo uso y valían para una sola compra cuyo importe debía ser superior al del bono pero, mediante una sencilla operación, podía conseguirse que ese bono pudiese utilizarse para varias compras y además cuyos importes fueran menores incluso que el precio del bono (con lo que el precio total podía ser negativo o 0 "cero").

Por tanto esos bonos, una vez descubierta la forma de tratarlos, podían tener "vida ilimitada".

Al final se descubrió la anomalía (las cuentas no cuadraban) y mediante la dirección de entrega los estafadores fueron localizados.

## ATAQUE INFORMÁTICO : Juzgado de Instrucción nº 2 de Lorca [junio de 1998]

Juzgado de Instrucción nº 2 de Lorca

Procedimiento Abreviado 1527/99

### A U T O

En Lorca a veintinueve de enero de dos mil dos.

### H E C H O S

PRIMERO.- El presente procedimiento se incoó por supuesto delito de descubrimiento y revelación de secretos en virtud de solicitud de mandamiento de entrada y registro interesado por oficio 94/99 de la Guardia Civil, Grupo de Delitos de alta Tecnología, de 8 de julio de 1999.

SEGUNDO.- Practicadas las primeras diligencias de instrucción, entre ellas la de entrada y registro aludidas y declaración de imputado, se acumularon a las presentes las diligencias previas que habían sido seguidas en el Juzgado de Instrucción nº 8 de Madrid bajo el número de autos 2481/99. Por último se practicaron determinadas diligencias de instrucción de carácter pericial informático y testifical del Ilmo. Sr. Subsecretario del Ministerio del Interior.

## RAZONAMIENTOS JURÍDICOS

PRIMERO.- Las presentes diligencias se incoaron en virtud de atestado de la Guardia Civil e informe del Ministerio del Interior de los que, resultaba la existencia de un ataque informático a los ordenadores del ministerio y la posible sustracción de dos ficheros, /etc/host y /etc/passwd. De la impecable investigación efectuada por el Grupo de delincuencia informática de la Unidad Central Operativa de la Guardia Civil se identificó al supuesto autor de los hechos que resultó ser D. O. C.. Los tipos delictivos en que se podrían haber sido inculcados, en principio, tales conductas serían los de descubrimiento y revelación de secretos del artículo 197 del Código Penal. Debe descartarse el delito de traición previsto y penado en los artículos 583.4º y 584 del CP al descartarse cualquier referencia de suministro de datos al "enemigo", "potencia extranjera", "asociación u organización internacional" como exigen tales preceptos. También debe descartarse la existencia de un delito relativo a la defensa nacional previsto y penado en los artículos 598 y siguientes del CP, pues de la declaración testifical practicada por el Subsecretario del Ministerio del Interior no resulta que la información a la que presuntamente se pretendió tener acceso fuera "información legalmente calificada como reservada o secreta, relacionada con la seguridad nacional o la defensa nacional". En cuanto a los tipos de descubrimiento y revelación de secretos definidos en el artículo 197 del Código Penal puede descartarse también el previsto en su párrafo segundo, pues se refiere a "datos reservados de carácter personal o familiar de otro" y ni en la página web del Ministerio del Interior ni en los ficheros cuya sustracción presuntamente se intentó figuran datos de esa naturaleza.

SEGUNDO.- El párrafo primero del artículo 197 castiga al que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apoderare de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus comunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación. Este delito ha sido calificado por la doctrina, en cuanto a su naturaleza, como un delito mutilado en dos actos, de tal forma que se realiza una acción como base para un actuar posterior del mismo sujeto activo, produciéndose la consumación tan pronto se realiza la primera acción, integrando la segunda acción el elemento subjetivo del injusto, en este caso, el ánimo de descubrir secretos. Es por ello que las conductas de mero "hacking" acceso a los sistemas informáticos perpetrados con la única finalidad de acceder al password o puerta lógica no son actualmente constitutivos de delito pues carecen del elemento subjetivo del injusto. En el caso de autos a la duda sobre la finalidad perseguida por D. O. C. cuando supuestamente trató de acceder y copiar los ficheros duda que siempre debe operar "in

dubio pro reo" se une la falta de acreditación suficiente de que dicho acceso tuviera éxito. En efecto, los diferentes atestados de la Guardia Civil, basados en la información suministrada por el propio Ministerio, no aclaran suficientemente si hubo o no sustracción de ficheros. El llamado "ataque coordinado masivo" a los ordenadores del Ministerio no resultó ser tal (atestado 64/98 e informe declaración del Sr. L. P. en relación con el ordenador "bisonte") no constando en modo alguno que el imputado actuara en connivencia con nadie. El informe realizado por el Departamento de microinformática de la Guardia Civil sobre el disco duro del ordenador personal intervenido al llamado "ministeriorrr" donde aparece un escudo de España, que aparte no ser significativo, su fecha de creación es de 7 de agosto de 1998, posterior a los hechos denunciados. El informe pericial por el profesor J. L. F. G. permite sostener que no queda rastro informático del que pueda inferirse que hubo intento de sustraer el fichero /etc/passwd. En cuanto al otro fichero /etc/hosts, parece que si hubo un intento fallido, pero ello no significa necesariamente que tuviera que conocerse su contenido, como exige el tipo delictivo, y en cualquier caso dicho fichero no contiene información secreta. Por último, la testifical del responsable del Ministerio del Interior es sumamente ilustrativa, pues reconoce que el ataque informático se produjo en la página web del Ministerio( de libre y general acceso), que a través de ella no podía tenerse acceso a las bases de datos, ratificando su versión contenida en el diario El País de que de haber tenido éxito la acción no hubiera pasado de una simple "gamberrada" y que quizá se hubiera producido "un poco de exceso en la calificación jurídica". Así pues, las actuaciones practicadas acreditan que el hecho denunciado no reviste caracteres de infracción criminal por lo que, de acuerdo con lo dispuesto en el artículo 637.2 y en la regla primera, inciso primero del artículo 789-5 de la Ley de Enjuiciamiento Criminal, procede acordar el SOBRESEIMIENTO LIBRE Y EL ARCHIVO de las mismas.

#### PARTE DISPOSITIVA

SE DECRETA EL SOBRESEIMIENTO LIBRE Y EL ARCHIVO DE LAS PRESENTES DILIGENCIAS.

Póngase esta resolución en conocimiento del Ministerio Fiscal y demás partes personadas, previniéndoles que contra la misma podrán interponer, ante este Juzgado, recurso de reforma y/o apelación, en el plazo de TRES DIAS.

Así lo acuerda, manda y firma D. ANTONIO ALCAZAR FAJARDO, MAGISTRADO JUEZ del Juzgado de Instrucción nº 2 de LORCA y su partido.- Doy fe.

#### FRAUDE EN ESPAÑA:

Implicados:  
BANESTO  
SISTEMA 4B  
PAGINAS AMARILLAS TPI  
RUTA 66 (León)

J.M.G.R. (Algeciras)  
E.R.W. (Salinas, California)

Hechos:

04.11.99: Ruta 66, establecimiento dedicado a la venta de motocicletas y ciclomotores firma con páginas amarillas tpi contrato para la apertura de comercio electrónico on-line.

29.12.99: Ruta 66 firma con Banesto un "contrato de comercio electrónico" para el cobro de las futuras operaciones originadas desde la tienda virtual en paginas-amarillas on-line.

27.06.00: Ruta 66 recibe un pedido desde Algeciras para un ciclomotor a través de internet.

27.06.00: Se recibe de "Banesto electronic payment system" formulario en los siguientes términos: transacción aprobada. Comercio:Ruta66. Importe: 307864. Referencia:gsmz9386 autorización nº:207777.

30.06.00: Se refleja en la cuenta que Ruta66 mantiene en Banesto el abono del importe de la compra, menos una pequeña cantidad sin justificar. (nos ingresan sólo 295.180 ptas.)

03.07.00: Se envía mediante empresa de transportes el vehículo al cliente en Algeciras, recibiendo éste la mercancía en perfecto estado.

30.09.00: Sistema 4b s.a. emite a Banesto una orden de retroceso de la operación realizada el día 27.06.00 por Ruta66 debido a que "...carece de la impresión de la tarjeta o la firma del titular..." y por un importe de 316.543 ptas. No coincidiendo con lo abonado inicialmente.(295.180) se adjunta un comunicado del titular de la tarjeta con la que se realizó el pago resultando que no es la misma persona que ha efectuado la compra. De la ciudad de salinas, en el estado de california (EE.UU) en el sentido de que alguien estaba utilizando sin su consentimiento el nº de la tarjeta Mastercard.

16.10.00: Banesto comunica a un responsable de ruta66 , de palabra, la existencia de una incidencia y le muestra la nota de adeudo de sistema 4b.

18.10.00: Solicitud denegada de cancelación de cuenta en Banesto.

19.10.00: Banesto efectúa un cargo en la cuenta de Ruta66 por un importe de 316.543 ptas. Y se niega a cancelar la cuenta al haber quedado ésta en descubierto.

24.10.00: El Servicio de Atención al cliente de Banesto, envía una carta y las condiciones generales.

31.10.00: Carta enviada por Ruta 66 al servicio de atención al cliente de Banesto

Conclusiones:

-La persona de Algeciras obtiene un ciclomotor mediante fraude en la utilización de tarjeta de crédito.

-La persona de Salinas (California) sufre inconvenientes, producto del citado fraude, pero ve restablecida su cuenta corriente.

-Sistema 4b retrocede un importe superior al previamente abonado y, a pesar de no haber verificado la titularidad del cliente, no asume responsabilidad alguna.

-Banesto se auto proclama como mero intermediario y despoja de validez a una autorización numerada y con referencias muy concretas, cargando en cuenta corriente un importe superior al saldo disponible en ese momento y pasando, a continuación, a reclamar el importe del descubiero más gastos.

-Paginas amarillas on-line como alojamiento de tiendas virtuales o galería comercial electrónica descubre que las condiciones y seguridad de los sistemas de pago concertados con Banesto son, cuando menos, imprevisibles y que, para los comerciantes, las ventas son un auténtico riesgo.

-Ruta66 sigue, en todo momento, los procedimientos y se queda sin el ciclomotor, sin el importe cobrado inicialmente, sin otro pequeño importe que no se ha podido justificar y sin explicaciones.

### EL FRAUDE DE LAS SUBASTAS ONLINE, LÍDER DE LOS CIBERCRÍMENES

El fraude en subastas realizadas a través de Internet supone el 87% de los incidentes criminales en Internet, según un estudio presentado por eMarketer.

En el estudio “ePrivacy & Security Report” también se destaca que el 34% de los usuarios de Internet han sido documentados por alguna infracción de seguridad o privacidad en la web.

Otro de los datos aportados por el estudio es que cada transacción fraudulenta en la Red cuesta unos 600\$, lo que supera la media estimada de gasto online. EMarketer añade que la mitad de los usuarios afectados por el fraude online son parte de la “Generación X” o baby boomers, dos de las poblaciones más extendidas en el mundo online. “Para muchos usuarios de Internet, la protección de información personal es una preocupación real y válida”, dice eMarketer. “Las ofertas de servicios gratuitos y promesas de grandes acuerdos incitan a los usuarios a consumir productos que jamás llegan o no cumplen la calidad prometida”.

El ratio de robos de tarjetas de crédito, como porcentaje del total de transacciones online realizadas, ha resultado ser extremadamente bajo, según eMarketer. Citando datos de Visa y MasterCard, el informe afirma que 22 millones de operaciones fraudulentas se realizaron en 1999, tanto online como offline, de un total de 25.000

millones de transacciones. Las subastas online podrían ver aumentado el porcentaje de fraudes debido al alto crecimiento esperado del sector de subastas entre particulares.

Se espera que las ventas generadas por las subastas online alcancen los 15.000 millones de dólares desde los 3.000 millones generados en 1999. En las últimas semanas, eBay, el líder del sector de subastas online, ha tomado medidas para evitar el fraude en su web. A finales de diciembre se afirmó que los acuerdos offline entre miembros serían prohibidos debido a que las transacciones realizadas de esta forma no recogían las medidas de seguridad de eBay y no están protegidas por el seguro de la compañía.

Los vendedores que acepten tratos offline serán primero avisados y posteriormente bloqueados si continúan sus actividades. Otros estudios confirman los datos que afirman que las subastas online generan la mayor parte de los fraudes en Internet. Un estudio de noviembre de la National Consumers League se manifiesta en términos similares al de eMarketer, y la FTC también ha avisado de los riesgos de estas subastas. Como nota positiva, la NCL afirma que los fraudes en subastas online están en descenso. Según la NCL, el 79% de las quejas producidas en el 2000 se referían a subastas, en contraste con el 87% que generó en 1999.

A continuación se exponen algunas NOTICIAS reales relacionadas con el tema de seguridad informática y más concretamente con las estafas:

#### INFORME SOBRE EL FRAUDE EN INTERNET [16-04-02]

El pasado año, el fraude en Internet ha costado 18 millones de dólares a 10.000 americanos, según se desprende de un estudio realizado por Internet Fraud Complaint Center.

Casi la mitad de los casos investigados en el informe están relacionados con las subastas online. Otras estafas incluían la no entrega de los productos o el fraude de tarjetas de crédito. La media de las pérdidas se situó en 435 dólares.

En opinión de Richard Johnston, director de Internet Fraud Complaint Center, las perspectivas no son halagüeñas. Sus estimaciones apuntan que las reclamaciones aumentarán de forma que pasarán de 1.000 a la semana a 1.000 diarias en el siguiente año, en la medida que dicha institución sea más conocida.

#### DETIENEN A UN "CRACKER" QUE UTILIZÓ EL "SITE" DE UN ANTIGUO EMPLEADO SUYO PARA PEDIR DINERO [18-05-02]

Daniel Aragay, vecino de Terrassa y propietario de Eurofestival.net ha explicado que el cracker "saqueó la página". La víctima ha dicho: "Hacerlo, le resultó bastante fácil porque sólo tuvo que contactar con Terra, un servidor de Telefónica, dar mi correo electrónico y decir que había perdido la contraseña". Al cabo de pocos días, Telefónica

le envió al detenido "no una sino tres veces, porque las dos primeras fueron retornadas, la contraseña por correo certificado". Con estos datos, el atacante pudo entrar en la página, poner una noticia que explicaba que la web había sido cerrada por problemas económicos y anunciar una cuenta corriente del Banco Bilbao Vizcaya, en la que se podía ingresar dinero para subsanar estos problemas.

"Spam" para robar datos sensibles [18-05-02]

Todos los usuarios de Internet hemos recibido en alguna ocasión mensajes de correo electrónico no solicitados de alguien que no conocíamos, la mayoría de las veces con anuncios y publicidad. Este tipo de mensajes enviados de forma masiva e indiscriminada es lo que denominamos "correo basura" o "spam". En los últimos tiempos hemos podido observar como prolifera esta vía para hacer llegar mensajes que, mediante engaños, tratan de robar información sensible del usuario, como contraseñas y datos de tarjetas de crédito.

En el ataque

La versatilidad del correo electrónico a través de Internet, como toda tecnología, puede utilizarse con distintos fines. Hace apenas una semana se ha distribuido un "spam" masivo que bajo el asunto "An Urgent notice from eBay Safe Harbor !", simulaba ser un aviso a los usuarios registrados del popular sitio eBay. El mensaje fraudulento notifica que los datos de nuestra cuenta de eBay deben ser actualizados por encontrarse erróneos o corruptos, para lo cual facilita un enlace a un formulario web que deberemos rellenar para que no se nos interrumpa el servicio.

Para darle más credibilidad, la dirección de remite aparece como "Safe Harbor" , mientras que a lo largo del mensaje hace referencia a que se utiliza SSL para que los datos transferidos viajen de forma segura, así como todo tipo de garantías sobre privacidad avalada por terceros. Una vez llegamos al formulario, mediante una URL encabezada por la IP del servidor, para intentar ocultar que el dominio no pertenece en realidad a eBay, nos encontramos con el citado formulario que simula el interfaz de eBay (logos, etc).

Por descontado, toda la información que se introduzca llegará a las manos del atacante, que podrá utilizarla para suplantar la identidad de los usuarios de eBay o realizar compras en otros sitios con los datos de sus tarjetas de crédito.

#### VULNERABILIDAD EN EL FILTRADO DE EMAIL DE ZONEALARM [08-04-02]

Se ha descubierto una vulnerabilidad en la característica MailSafe de ZoneAlarms por la cual un atacante puede saltarse la protección de filtrado de archivos adjuntos.

ZoneLabs ZoneAlarm es una conocida aplicación de cortafuegos personal para sistemas Windows muy popular en entornos domésticos. Entre las diversas funcionalidades que aporta se incluye MailSafe que aporta características de filtrado de contenido para bloquear mensajes con determinadas características.

Se ha anunciado una vulnerabilidad en la característica MalSafe de ZoneAlarm por la cual un atacante puede evitar el bloqueo de archivos con una determinada extensión (por ejemplo archivos .exe). Si el archivo se envía con un punto adicional (".") al nombre completo el archivo no será bloqueado.

ZoneLabs ha solucionado este problema para lo que se recomienda emplear la característica "Check for Update" del firewall.

# LA AUDITORÍA INFORMÁTICA

## INTRODUCCIÓN

A finales del siglo XX, los Sistemas Informáticos se han constituido en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial, los Sistemas de Información de la empresa.

La Informática hoy, está totalmente incluida en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar, por lo tanto, sometidos a las disposiciones generales de las leyes. En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado el "management" o gestión de la empresa. Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma. Pero aún así, debido a su importancia en el funcionamiento de una empresa, existe la Auditoría Informática.

El término de Auditoría se ha empleado incorrectamente con frecuencia ya que se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallos. El concepto de auditoría es mucho más que esto. **Es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una sección, un organismo, una entidad, etc.**

Cabe destacar que la auditoría es un examen crítico pero no mecánico, que no implica la preexistencia de fallos en la entidad auditada y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo.

Los principales objetivos que constituyen la auditoría Informática son el control de la función informática, el análisis de la eficiencia de los Sistemas Informáticos que comporta, la verificación del cumplimiento de la Normativa general de la empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos informáticos.

La importancia de llevar un control de esta los sistemas informáticos se puede deducir de varios aspectos. He aquí algunos:

- Las computadoras y los Centros de Proceso de Datos se convirtieron en blancos apetecibles no solo para el espionaje, sino para la delincuencia y el terrorismo. En este caso interviene la Auditoría Informática de Seguridad (la que más nos preocupa en el objetivo de este trabajo).
- Las computadoras creadas para procesar y difundir resultados o información elaborada pueden producir resultados o información errónea si dichos datos son, a su vez, erróneos. Este concepto obvio es a veces olvidado por las mismas empresas que terminan perdiendo de vista la naturaleza y calidad de los datos de entrada a sus Sistemas Informáticos, con la posibilidad de que se provoque un efecto cascada y afecte a Aplicaciones independientes. En este caso interviene la Auditoría Informática de Datos.

- Un Sistema Informático mal diseñado puede convertirse en una herramienta harto peligrosa para la empresa: como las maquinas obedecen ciegamente a las órdenes recibidas y la modelización de la empresa está determinada por las computadoras que materializan los Sistemas de Información, la gestión y la organización de la empresa no puede depender de un Software y Hardware mal diseñados. De esto se encargaría la Auditoría Informática de Sistemas.

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También puede ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus. El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica.

La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.

La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

La seguridad informática se la puede dividir como Área General y como Área Especifica (seguridad de Explotación, seguridad de las Aplicaciones, etc.). Así, se podrán efectuar auditorías de la Seguridad Global de una Instalación Informática – Seguridad General- y auditorías de la Seguridad de un área informática determinada – Seguridad Especifica -.

Con el incremento de agresiones a instalaciones informáticas en los últimos años, se han ido originando acciones para mejorar la Seguridad Informática a nivel físico. Los accesos y conexiones indebidos a través de las Redes de Comunicaciones, han acelerado el desarrollo de productos de Seguridad lógica y la utilización de sofisticados medios criptográficos.

El sistema integral de seguridad debe comprender:

- Elementos administrativos
- Definición de una política de seguridad
- Organización y división de responsabilidades

- Seguridad física y contra catástrofes (incendio, terremotos, etc.)
- Prácticas de seguridad del personal
- Elementos técnicos y procedimientos
- Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.
- Aplicación de los sistemas de seguridad, incluyendo datos y archivos
- El papel de los auditores, tanto internos como externos
- Planeación de programas de desastre y su prueba.

La decisión de abordar una Auditoría Informática de Seguridad Global en una empresa, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que está sometida elaborando una serie de prioridades en las que se tendrán en cuenta los aspectos más importantes de una empresa.

### PASOS DE UNA AUDITORÍA INFORMÁTICA DE SEGURIDAD

A pesar de la poca información de la que se dispone sobre este campo, nosotros hemos decidido sugerir una metodología ya existente modificando algún pequeño aspecto. Esta metodología para realizar una auditoría informática sobre la seguridad de una empresa es la metodología CRMR (Computer resource management review) o traducido de una forma más adecuada, Evaluación de la Gestión de Recursos Informáticos. Esta terminología quiere destacar la posibilidad de realizar una evaluación de eficiencia de utilización de los recursos por medio de la gestión, no teniendo el grado de profundidad de una auditoría global, pero sí proporcionando soluciones rápidas y eficaces a problemas concretos.

La Auditoría de Seguridad Informática es una auditoría que tiene como misión revisar tanto la seguridad física del Centro de Proceso de Datos en su sentido más amplio, como la seguridad lógica de datos, procesos y funciones informáticas más importantes de aquél.

El objetivo de esta auditoría de seguridad es revisar la situación y las cuotas de eficiencia de la misma en los órganos más importantes de la estructura informática. Para ello, se fijan los supuestos de partida:

El área auditada es la Seguridad. Se podría dividir esta área en varios segmentos para que su análisis fuese más concreto en los distintos puntos:

- Segmento 1: Seguridad de cumplimiento de normas y estándares.
- Segmento 2: Seguridad de Sistema Operativo.
- Segmento 3: Seguridad de Software.
- Segmento 4: Seguridad de Comunicaciones.
- Segmento 5: Seguridad de Base de Datos.
- Segmento 6: Seguridad de Proceso.
- Segmento 7: Seguridad de Aplicaciones.
- Segmento 8: Seguridad Física.

Se darán los resultados globales de todos los segmentos y se realizará un tratamiento exhaustivo del Segmento 8, el cual se descompondrá a su vez en varios subsegmentos debido a que éste es un campo bastante importante y que abarca diversas secciones.

Conceptualmente la auditoría informática en general y la de Seguridad en particular, ha de desarrollarse en seis fases bien diferenciadas:

**Fase 0.** Causas de la realización del ciclo de seguridad.

**Fase 1.** Estrategia y logística del ciclo de seguridad.

**Fase 2.** Ponderación de sectores del ciclo de seguridad.

**Fase 3.** Operativa del ciclo de seguridad.

**Fase 4.** Cálculos y resultados del ciclo de seguridad.

**Fase 5.** Confección del informe del ciclo de seguridad.

#### Fase 0. Causas de realización de una Auditoría de Seguridad

Esta es lo primero que se debería hacer al comenzar una auditoría.

El equipo auditor debe conocer las razones por las cuales el cliente desea realizar el Ciclo de Seguridad. Puede haber muchas causas: Reglas internas del cliente, incrementos no previstos de costes, obligaciones legales, situación de ineficiencia global notoria, etc.

De esta manera el auditor conocerá el entorno inicial para poder elaborar así el Plan de Trabajo.

#### Fase 1. Planificación del ciclo de Seguridad

Se desarrolla en las siguientes actividades:

1. Designación del equipo auditor.
2. Asignación de interlocutores, validadores y decisores del cliente.
3. Cumplimentación de un formulario general por parte del cliente, para la realización del estudio inicial.

Con las razones por las cuales va a ser realizada la auditoría (Fase 0), el equipo auditor diseña el proyecto de Ciclo de Seguridad con arreglo a una estrategia definida en función del volumen y complejidad del trabajo a realizar, que constituye la Fase 1 del punto anterior.

Para desarrollar la estrategia, el equipo auditor necesita recursos materiales y humanos. La adecuación de estos se realiza mediante un desarrollo logístico, en el que los mismos deben ser determinados con exactitud. La cantidad, calidad, coordinación y distribución de los mencionados recursos, determina a su vez la eficiencia y el precio del Proyecto.

Los planes del equipo auditor se desarrolla de la siguiente manera:

1. Eligiendo el responsable de la auditoria su propio equipo de trabajo. Este ha de ser heterogéneo en cuanto a las especialidades que manejen los miembros, pero compacto.
2. Recabando de la empresa auditada los nombres de las personas de la misma que han de relacionarse con los auditores, para las peticiones de información, coordinación de entrevistas, etc.
3. Mediante un estudio inicial, del cual forma parte el análisis de un formulario exhaustivo, también inicial, que los auditores entregan al cliente para su cumplimentación.

Según los planes marcados, el equipo auditor, cumplidos los requisitos 1, 2 y 3, estará en disposición de comenzar con lo que será en sí la auditoría.

### Fase 2. Ponderación de los Sectores Auditados

Engloba las siguientes actividades:

1. Asignación de pesos técnicos. Se entienden por tales las ponderaciones que el equipo auditor hace de los segmentos y secciones, en función de su importancia.
2. Asignación de pesos políticos. Son las mismas ponderaciones anteriores, pero evaluadas por el cliente.
3. Asignación de pesos finales a los Segmentos y Secciones. El peso final es el promedio del peso técnico y del peso político.

Se pondera la importancia relativa de la seguridad en los diversos sectores de la organización informática auditada.

<b>Ciclo de Seguridad. Suma Pesos Segmentos = 100</b> (con independencia del número de segmentos consideradas)			
Segmentos	Pesos Técnicos	Pesos Políticos	Pesos Finales
Seg1. Normas y Estándares	12	8	10
Seg2. Sistema Operativo	10	10	10
Seg3. Software Básico	10	14	12
Seg4. Comunicaciones	12	12	12
Seg5. Bases de Datos	12	12	12
Seg6. Procesos	16	12	14
Seg7. Aplicaciones	16	16	16
Seg8. Seguridad Física	12	16	14
<b>TOTAL</b>	<b>100</b>	<b>100</b>	<b>100</b>

<b>Suma Peso Secciones = 20</b> (con independencia del número de Secciones consideradas)			
Secciones	Pesos Técnicos	Pesos Políticos	Pesos Finales
Sec1. Seg. Física de	6	6	6

Datos			
Secc2. Control de Accesos	5	3	4
Secc3. Equipos	6	4	5
Secc4. Documentos	2	4	3
Secc5. Suministros	1	3	2
TOTAL	20	20	20

Las secciones serán las partes en las que se podrá dividir cada segmentos en función de las tareas que cumpla cada uno.

### Fase 3. Análisis profundo de la empresa

Una vez asignados los pesos finales a todos los Segmentos y Secciones, se comienza la Fase 3, que implica las siguientes actividades:

1. Preparación y confirmación de entrevistas.
2. Entrevistas, pruebas, análisis de la información, cruzamiento y repaso de la misma.

Las entrevistas deben realizarse con exactitud. El responsable del equipo auditor designará a un encargado, dependiendo del área de la entrevista. Este, por supuesto, deberá conocer a fondo la misma.

La realización de entrevistas adecuadas constituye uno de los factores fundamentales del éxito de la auditoría. La adecuación comienza con la completa cooperación del entrevistado.

Deben realizarse varias entrevistas del mismo tema, al menos a dos o tres niveles jerárquicos distintos. El mismo auditor puede, y en ocasiones es conveniente, entrevistar a la misma persona sobre distintos temas. Las entrevistas deben realizarse de acuerdo con el plan establecido, aunque se pueden llegar a agregar algunas adicionales y sin planificación.

Comenzada la entrevista, el auditor o auditores formularán preguntas al/los entrevistado/s identificando quien ha dicho qué, si son más de una las personas entrevistadas.

Las Checklist's (baterías de preguntas sobre un tema) son útiles y en muchos casos imprescindibles. Terminadas las entrevistas, el auditor califica las respuestas del auditado (no debe estar presente) y procede al levantamiento de la información correspondiente.

Simultáneamente a las entrevistas, el equipo auditor realiza pruebas planeadas y pruebas sorpresa para verificar y cruzar los datos solicitados y facilitados por el cliente. Estas pruebas se realizan ejecutando trabajos propios o repitiendo los de aquél, que indefectiblemente deberán ser similares si se han reproducido las condiciones de carga de los Sistemas auditados. Si las pruebas realizadas por el equipo auditor no fueran consistentes con la información facilitada por el auditado, se deberá recabar nueva información y reverificar los resultados de las pruebas auditoras.

La evaluación de las Checklists, las pruebas realizadas, la información facilitada por el cliente y el análisis de todos los datos disponibles, configuran todos los elementos necesarios para calcular y establecer los resultados de la auditoría, que se materializarán en el informe final.

Este podría ser un pequeño ejemplo de las típicas preguntas que se podrían realizar a un empleado del área de control de accesos de una empresa en una subsección de autorizaciones que forma parte del segmento 8.

Control de Accesos: <b>Autorizaciones</b>		
Preguntas	Respuestas	Puntos
¿Existe un único responsable de implementar la política de autorizaciones de entrada en el Centro de Cálculo?	Si, el Jefe de Explotación, pero el Director puede acceder a la Sala con acompañantes sin previo aviso.	4
¿Existe alguna autorización permanente de estancia de personal ajeno a la empresa?	Una sola. El técnico permanente de la firma suministradora.	5
¿Quiénes saben cuales son las personas autorizadas?	El personal de vigilancia y el Jefe de Explotación.	5
Además de la tarjeta magnética de identificación, ¿hay que pasar otra especial?	No, solamente la primera.	4
¿Se pregunta a las visitas si piensan visitar el Centro de Cálculo?	No, vale la primera autorización.	3
¿Se preveen las visitas al Centro de Cálculo con 24 horas al menos?	No, basta que vayan acompañados por el Jefe de Explotación o Director	3
<b>TOTAL AUTORIZACIONES</b>		<b>24/30 80%</b>

#### Fase 4. Cálculos y Resultados del Ciclo de Seguridad

1. Cálculo y ponderación de Secciones y Segmentos. Las Subsecciones no se ponderan, solo se calculan.
2. Identificación de materias mejorables.
3. Priorización de mejoras.

El trabajo de levantamiento de información está concluido y contrastado con las pruebas. A partir de ese momento, el equipo auditor tiene en su poder todos los datos necesarios para elaborar el informe final.

Una vez realizado los cálculos, se ordenaran y clasificaran los resultados obtenidos por materias mejorables, estableciendo prioridades de actuación para lograrlas.

*Cálculo del ejemplo de las Subsecciones de la Sección de Control de Accesos:  
Autorizaciones 80%*

Controles Automáticos 70%  
 Vigilancia 70%  
 Registros 30%  
 Promedio de Control de Accesos 62,5%

Después habrá que tener en cuenta el peso técnico de la sección del Control de Accesos declarados en el punto 2.

Prosiguiendo con el ejemplo, se procedió a la evaluación de otras cuatro Secciones, obteniéndose los siguientes resultados:

Ciclo de Seguridad: <b>Segmento 8, Seguridad Física.</b>		
Secciones	Peso	Puntos
Sección 1. Datos	6	57,5%
Sección 2. Control de Accesos	4	62,5%
Sección 3. Equipos (Centro de Cálculo)	5	70%
Sección 4. Documentos	3	52,5%
Sección 5. Suministros	2	47,2%

Conocidas los promedios y los pesos de las cinco Secciones, se procede a calcular y ponderar el Segmento 8 de Seguridad Física:

$$\text{Seg. 8} = \text{PromedioSección1} * \text{peso} + \text{PromedioSecc2} * \text{peso} + \text{PromSecc3} * \text{peso} + \text{PromSecc4} * \text{peso} + \text{PromSecc5} * \text{peso} / (\text{peso1} + \text{peso2} + \text{peso3} + \text{peso4} + \text{peso5})$$

A continuación, la evaluación final de los demás Segmentos del ciclo de Seguridad:

Ciclo de Seguridad. Evaluación y pesos de Segmentos		
Segmentos	Pesos	Evaluación
Seg1. Normas y Estándares	10	61%
Seg2. Sistema Operativo	10	90%
Seg3. Software Básico	12	72%
Seg4. Comunicaciones	12	55%
Seg5. Bases de Datos	12	77,5%
Seg6. Procesos	14	51,2%
Seg7. Aplicaciones	16	50,5%
Seg8. Seguridad Física	14	59,8%
<b>Promedio Total Area de Seguridad</b>	<b>100</b>	<b>63,3%</b>

Se han tenido en cuenta los siguientes puntos a la hora de evaluar los resultados producidos:

- a. Valoración de las respuestas a las preguntas específicas realizadas en las entrevistas y a los cuestionarios formulados por escrito.
- b. Cálculo matemático de todas las subsecciones de cada sección, como media aritmética (promedio final) de las preguntas específicas. Recuérdese que las subsecciones no se ponderan.

- c. Cálculo matemático de la Sección, como media aritmética (promedio final) de sus Subsecciones. La Sección calculada tiene su peso correspondiente.
- d. Cálculo matemático del Segmento. Cada una de las Secciones que lo componen se afecta por su peso correspondiente. El resultado es el valor del Segmento, el cual, a su vez, tiene asignado su peso.
- e. Cálculo matemático de la auditoría. Se multiplica cada valor de los Segmentos por sus pesos correspondientes, la suma total obtenida se divide por el valor fijo asignado a priori a la suma de los pesos de los segmentos.

Finalmente, se procede a mostrar las áreas auditadas con gráficos de barras, exponiéndose primero los Segmentos, luego las Secciones y por último las Subsecciones. En todos los casos se referenciarán respecto a tres zonas de distintos colores.

La primera zona corresponde a una situación de debilidad que requiere acciones a corto plazo. Serán las más prioritarias, tanto en la exposición del Informe como en la toma de medidas para la corrección.

La segunda corresponde a una situación discreta que requiere acciones a medio plazo, figurando a continuación de las contenidas en la zona roja.

La tercera requiere solamente alguna acción de mantenimiento a largo plazo.

#### Fase 5. Confección del Informe del Ciclo de Seguridad

1. Preparación de borrador de informe y Recomendaciones.
2. Discusión del borrador con el cliente.
3. Entrega del Informe y Carta de Introducción.

Ha de resaltarse la importancia de la discusión de los borradores parciales con el cliente. La referencia al cliente debe entenderse como a los responsables directos de los segmentos. Es de destacar que si hubiese acuerdo, es posible que el auditado redacte un contrainforme del punto cuestionado.

Las Recomendaciones del Informe son de tres tipos:

1. Recomendaciones correspondientes a la primera zona. Serán muy detalladas e irán en primer lugar, con la máxima prioridad. La redacción de las recomendaciones se hará de modo que sea simple verificar el cumplimiento de la misma por parte del cliente.
2. Recomendaciones correspondientes a la segunda. Son las que deben observarse a medio plazo, e igualmente irán priorizadas.
3. Recomendaciones correspondientes a la tercera. Suelen referirse a medidas de mantenimiento. Pueden ser omitidas. Puede detallarse alguna de este tipo cuando una acción sencilla y económica pueda originar beneficios importantes.

Este sería el plan de realización de una auditoría de seguridad que nosotros recomendamos teniendo en cuenta que habría que adaptarlo para cada tipo de empresa y no basándose en los ejemplos que adjuntamos puesto que estos solo servirían para grandes empresas. Para las pequeñas habría que examinar que áreas abarcan y cuáles son los métodos más apropiados para analizarlas, siempre siguiendo, como no, el método de evaluación de la metodología CRMR.

## CONCLUSIÓN

Incluir en el Código Penal, en el título Quinto del Libro Segundo, Capítulo 3 (Violación de secretos), y Capítulo 4 (Delitos contra la libertad de trabajo y asociación), los delitos cometidos a través de una computadora. Tipificando así en el primero de ellos los delitos de violación de correspondencia privada recibida a través de la computadora

(e-mail) ya sea de empresas públicas o privadas.

En el segundo tipificando la competencia desleal.

Incluir en el Código Penal, en el título Sexto del Libro Segundo, Capítulo 3 (Extorsión) y Capítulo 4 (Estafas y otras defraudaciones) también los delitos cometidos a través de la computadora o a través del software. Legislar un tipo culposo para aquellos que, por imprudencia, negligencia, impericia causaren daños, introduzcan virus u otros, con capacidad de dañar a través de la computadora. Considerando culposa la conducta de

quien a través de la computadora daña los controles de un enfermo o paciente.

Legislar la instigación al delito cometido a través de la computadora.

Adherimos, por nuestra parte, a los postulados de la ONU sobre los delitos informáticos, con el fin de unificar la legislación internacional que regule la problemática de la cibernética y su utilización tan generalizada en el mundo.

Desde la Criminología debemos señalar que anonimato, sumado a la inexistencia de una norma que tipifique los delitos señalados, son un factor criminógeno que favorece la multiplicación de autores que utilicen los medios electrónicos para cometer delitos a sabiendas que no serán alcanzados por la ley.

Por otro lado hemos enumerado una serie de entretenimientos que tienen a un menor frente a una PC como víctima pasiva, incitado a la violencia, alejado de los procesos de socialización. Recordemos que el Congreso Panamericano de Criminología determinó en 1979, que se encuentra en estado de abandono el menor que no está en contacto con padres, abuelos o educadores, por más de cuatro horas.

## **BIBLIOGRAFÍA**

[www.delitosinformaticos.com](http://www.delitosinformaticos.com)

Estudio de la Lopd y su reglamento: Universidad de Castilla la Mancha

[www.gestipolis.com](http://www.gestipolis.com)

La protección de la propiedad intelectual de las organizaciones: Pedro Cardona Vilaplana.

LORTAD: Reglamento de seguridad. E. Del Peso Navarro, M.A. Ramos González

La información como activo estratégico: seguridad y protección: E. Del Peso Navarro

Seguridad Informática: CB Soft