Primer Informe sobre la necesidad legal de cifrar información y datos personales

Informe presentado por el Despacho de Abogados con especialización en tecnología y protección de datos:

ABANLEX

Colabora: SOPHOS

ÍNDICE

1 Cifrar de forma legal es accesible, fácil y posible

Cifrar datos de forma correcta es una de las obligaciones que impone la normativa española para una inmensa cantidad de empresas. Muchas de ellas no cifran por miedo o desconocimiento. Cifrar no es complicado, el coste es asequible y los beneficios se muestran desde el inicio.

"La idea de la dificultad en la aplicación de las Medidas de Seguridad en materia de Protección de Datos es una idea errónea y falaz", afirmó don Arturo Ribagorda, Catedrático de Informática de la Universidad Carlos III, según la nota informativa de la AEPD y la UCM publicada en 2006. El catedrático indicó que, ya en ese año, existían herramientas que permiten el cifrado de datos y la obtención de copias de respaldo "sin excesiva dificultad".

Hoy en día es más sencillo cifrar, que lo que era en 2006 cuando la AEPD formaba sobre la facilidad de la aplicación de las medidas de seguridad. Las herramientas de cifrado son cada vez más comunes, así como las empresas que desarrollan soluciones profesionales personalizadas para corporaciones y empresas de todos los tamaños.

2 Cifrar es el medio técnico correcto

Cifrar de forma correcta y siguiendo los parámetros indicados en la normativa española vigente es uno de los medios técnicos respaldados por las autoridades nacionales por el cual se garantiza la protección del derecho fundamental a la protección de datos, además de respaldar la seguridad de los valores de la empresa y otorgar confianza a los operadores del mercado.

El Gabinete Jurídico de la Agencia Española de Protección de Datos recuerda, en su Informe 494/2009, cuál es la importancia del cifrado correcto, de manera que sea legal y suficiente:

"*La seguridad en el intercambio de información de carácter personal en la que hay que adoptar medidas de seguridad de nivel alto, en particular los requisitos de cifrado de datos, no es un tema baladí, ni un mero trámite administrativo, ni una cuestión de comodidad.* ***Es el medio técnico por el cual se garantiza la protección de un derecho fundamental y al que hay que dedicar el tiempo y los recursos que sean necesarios para su correcta implementación***".

3 Quién está obligado a cifrar en España

Deben cifrar la información un gran número de empresas. Podríamos decir que deben hacerlo todos los sujetos que traten datos personales contenidos en ficheros a los que se deban aplicar medidas de seguridad de nivel alto. Sin embargo, el número es un poco más generoso, ya que debemos incluir también otro tipo de sujetos que realizan actividades que destacamos a continuación.

Deben cifrar datos los siguientes tipos sujetos y empresas:

- Los sujetos que tengan los siguientes ficheros de datos personales o realicen los tratamientos de datos de carácter personal que se indican: (art. 81.3 RLPOD):
  - Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
  - Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
  - Aquéllos que contengan datos derivados de actos de violencia de género.
- Los sujetos obligados al cumplimiento de la normativa de prevención del blanqueo de capitales y de la financiación del terrorismo (art. 2 Ley 10/201), respecto de determinados ficheros que están obligados a crear (art. 15 y 32 Ley 10/2010)

- Sujetos que gestionan ficheros de whistleblowers, respecto del conjunto ordenado de datos de carácter personal de alertadores y potenciales incumplidores (Informe AEPD)
- Abogados en el ejercicio de su profesión, respecto del fichero de clientes (arts. 18 y 24 CE y art. 5 Código Deontológico)
- Las Administraciones públicas en cumplimiento del Esquema Nacional de Seguridad (Anexos RD 3/2010)
- Empresas que adheridas a un Código Tipo que obligue al cifrado (art. 72 RLOPD)
- Empresas que aceptan el BYOD (CCN-CERT IA-21/13)
- Empresas que deseen proteger sus creaciones (art 1 LPI)
- Empresas que deseen proteger sus secretos comerciales (art. 13 LCD)
- Empresas que deseen proteger minimizar el espionaje industrial (art. 278, 279 y 280 CP)
- Empresas que deseen adoptar medidas de seguridad que superen el mínimo exigido (art. 81.7 RLPOD)

4 Requisitos que debe cumplir un cifrado legal

Cuando la normativa española exige cifrado, otorga a las empresas dos posibilidades (art. 104 RLOPD): Un sistemas de cifrado o cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Únicamente son válidos los sistemas de cifrado que garantizan que la información no sea inteligible ni manipulada por terceros. Cualquier sistema no es suficiente. ¿Pero cuáles son estos? ¿Quién los ha auditado? ¿Hay alguna lista de los que permiten cumplir la ley y los que no?

A la Agencia Española de Protección de Datos se le consultó si los sistemas de cifrados de ciertas herramientas, como las de compresión de archivos (ZIP) y los sistemas de claves de los PDF eran suficientes para cumplir la normativa. El Gabinete Jurídico de la Agencia Española de Protección de Datos, en su Informe 0494/2009, respondió: no son suficientes.

> **Artículo 104 del Reglamento de la LOPD**
>
> "*Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros*".

Existen técnicas, dice la Agencia, que actualmente se pueden emplear como alternativa al cifrado de datos, como son la esteganografía para el caso de ocultación de mensajes a nivel de aplicación o la transmisión mediante espectro ensanchado (spread-spectrum) para el caso inalámbrico a nivel físico. Todas ellas con una implementación y una gestión mucho más compleja y problemática que la que ofrecen los actuales sistemas de cifrado. En 2009 la Agencia afirmó que aún no se disponían de tecnologías más ágiles para preservar la confidencialidad de la información que emplear herramientas de cifrado, aunque en un futuro estas puedan aparecer.

Pero no sólo es necesario cifrar, sino cifrar de forma que la información no sea inteligible ni manipulada por terceros. Sin esta última condición, no se cumplirá lo estipulado en el citado artículo 104. Esto implica dos cosas:

- Por un lado que el sistema de cifrado a emplear no esté comprometido, es decir, que no se conozca forma de romperlo.
- Por otro lado, que se cuente con un sistema de gestión de claves, en particular, y con un procedimiento de administración de material criptográfico, en general.

Ante la pregunta de si los sistemas de cifrado de WinZip y PDF es suficiente, la Agencia contestó lo siguiente: "*Los pro-*

ductos que generan archivos PDF o el realizado por WinZip tienen vulnerabilidades conocidas y se disponen de herramientas de libre distribución que aprovechan dichas vulnerabilidades. Más concretamente, no sólo se pueden obtener en Internet fácilmente utilidades que rompen las protecciones de los archivos PDF o ZIP, sino que el propio algoritmo en el que descansa la cifra de documentos PDF, el algoritmo RC4, es manifiestamente vulnerable".

La Agencia concluye lo siguiente:

- Para un uso particular, los sistemas generales de cifrado (ZIP, PDF, etc.) podrían considerarse adecuados, según el caso.
- Para un uso profesional, los sistemas generales de cifrado son insuficientes para el intercambio de información con las garantías que se precisan en el Reglamento.

La respuesta para cumplir la normativa se encuentra en las herramientas profesionales pensadas, diseñadas y probadas para cumplir al detalle la normativa vigente en España en materia de cifrado.

5 La importancia de cifrar de forma legal

5.1 Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD).

El objeto de la LOPD es "*garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*" (art. 1 LOPD).

El principal efecto de esta norma (LOPD) es limitar 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*" (art. 18 CE). Uno de los pilares de la normativa de protección de datos es el asentamiento de medidas de seguridad para alcanzar el objeto indicado.

Las medidas de seguridad que marca la normativa de protección de datos se dividen en tres niveles: bajo, medio y alto. El que más interesa a los efectos de cifrado es el alto, que obliga a cifrar datos, sin desmerecer a los dos anteriores, que también podrán incorporar el cifrado de manera voluntaria.

Una de las bases que sustentan la necesidad del cifrado se encuentra en la obligación, que impone la LOPD, al secreto profesional y al deber de guardar los datos de carácter personal. Esta obligación recae sobre el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal.

Artículo 10 LOPD

"El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

El incumplimiento de estos deberes de secreto y custodia adecuada se considera una infracción grave. Las sanciones se califican como leves, graves o muy graves, siendo grave la vulneración del deber de guardar secreto, lo cual se sanciona con una multa de 40.001 a 300.000 euros.

Artículo 44.3 LOPD

"Son infracciones graves: [...] La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley."

Artículo 45.2 LOPD

"Las infracciones graves serán sancionadas con multa de 40.001 a 300.000 euros."

En caso de que el cifrado no se realice de forma correcta y los datos quedarán expuestos a terceras personas sin autorización para observarlos, se estaría llevando a cabo una cesión o comunicación pública de datos, definida en la LOPD como "*toda revelación de datos realizada a una persona distinta del interesado*" (Art. 3 LOPD).

La repercusión económica de la imposición de la sanción, de 40.001 a 300.000 euros, es considerable. Sin embargo, este importe no será el único que haya que pagar, ya que será complementado con el propio de la indemnización que, en su caso, haya que abonar a los damnificados por la fuga de datos y su exposición indebida.

Cuando la norma obliga a cifrar datos, el cifrado se debe realizar. Hay que dedicar el tiempo y los recursos que sean necesarios para su correcta implementación, como nos recuerda la Agencia en su Informe 494/2009 y como nos indica la propia LOPD en su articulado.

Artículo 9.1 LOPD

"***El responsable del fichero, y, en su caso, el encargado del tratamiento deben adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural***".

5.2 Reglamento de Desarrollo de la LOPD (RLOPD).

El objeto del Reglamento es desarrollar la LOPD. Es decir, fortalecer los mecanismos por los que se garantiza y protege, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Los sujetos obligados que tratan datos personales deben adoptar medidas adecuadas para limitar el acceso del personal a datos personales. En cuanto al personal ajeno, los sujetos obligados deben recoger de forma expresa en un contrato la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio. Estas obligaciones son aplicables a todo tipo de tratamiento de datos, desde el que requiere la aplicación de medidas de seguridad de nivel bajo hasta el que requiere las de nivel alto.

Cifrar fortalece la seguridad de la empresa y genera confianza en los trabajadores y en los clientes.

Artículo 83 RLOPD

"***El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.***

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio."

En relación con la necesidad de identificar y autenticar a los usuarios, el artículo 93 RLOPD exige al responsable del fichero o tratamiento que adopte las medidas necesarias para garantizar que estas acciones se realizan de forma correcta. Se le exige, en particular, establecer "*un mecanismo que permita la identificación de forma inequívoca y personalizada*" de los usuarios que intenten "*acceder al sistema de información*" y así como verificar que está autorizado. En caso de que el mecanismo de autenticación se base en la existencia de contraseñas, la norma no exige que estas se almacenen de forma cifrada, pero se extrae del literal de la norma la conveniencia de que se lleve a cabo un cifrado de las mismas, para garantizar su confidencialidad e integridad y, en particular, para que su almacenamiento mientras estén vigentes se realice de forma ininteligible. Por tanto, este es el primer elemento que hace necesario un sistema de cifrado para obligados que gestionen ficheros con medidas de nivel bajo: cifrado de contraseñas en vigor.

La primera referencia expresa a la obligación de cifrado la encontramos en el artículo 101 del RLOPD. El Reglamento obliga al cifrado de datos bajo las siguientes condiciones:

1. El cifrado de datos deberá garantizar que la información no sea accesible o manipulada.
2. Se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.
3. Se evitará el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado.

Artículo 101.2 y 101.3 RLOPD

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

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos."

Para comprender el siguiente punto en el que el Reglamento menciona expresamente la obligación de cifrado, debe recordarse a qué ficheros o tratamientos de datos de carácter personal se les debe aplicar las medidas de nivel alto, además de las del nivel bajo y medio. Según el artículo 81 RLOPD estos son: los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual; los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas; y aquéllos que contengan datos derivados de actos de violencia de género.

Cuando nos encontremos ante los referidos ficheros o tratamientos de datos de carácter personal, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará, indica el artículo 101 RLOPD, "*cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros*".

5.3 Ley de Autonomía del Paciente (Ley 41/2002).

El objeto de la Ley de Autonomía del Paciente es "*la regulación de los derechos y obligaciones de los pacientes, usuarios y profesionales, así como de los centros y servicios sanitarios, públicos y privados, en materia de autonomía del paciente y de información y documentación clínica*" (art. 1 Ley 41/2002).

Los ficheros que tratan los sujetos obligados por esta norma deben ser objeto de aplicación de nivel alto de medidas seguridad. Esto resulta en que el cifrado es directamente aplicable y obligatorio.

El principal motivo, además de los desgranados en la LOPD y su Reglamento de Desarrollo, se muestra en el artículo 2 de la norma, en el que se indica que toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y la documentación clínica debe ser orientada por "*la dignidad de la persona humana, el respeto a la autonomía de su voluntad y a su intimidad*". Estos derechos fundamentales hacen imprescindible el máximo celo a la hora de tratar la información concerniente a las personas físicas que serán atendidas por los sujetos obligados. El cifrado de los datos es una de las medidas esenciales a las que obliga la normativa de protección de datos. Asimismo, se impone la obligación, a la persona que elabora o tiene acceso a la información y la documentación clínica, de guardar la reserva debida. Esta obligación de guardar reserva se refuerza con un sistema adecuado de cifrado de datos que impida el envío por error de datos, que se compartan indebidamente o que se acceda a ellos en caso de extravío de uno de los soportes que los contienen.

El derecho a la intimidad de la persona es uno de los factores de mayor relevancia a la hora de llevar a cabo cifrados adecuados y conformes a la normativa.

Para preservar de forma correcta los derechos de los pacientes, con especial referencia a su intimidad, el artículo 16 de la Ley 41/2002 es claro al determinar que "*el acceso a los datos*" debe de realizarse, en todo caso, por un "*profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto*". De igual forma, "*el personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto*". Este deber de secreto unido a la salvaguarda efectiva del derecho fundamental hacen imprescindible el recurso al cifrado de datos, obligatorio, por otro lado, por el tipo de datos que van a ser tratados y la implantación debida de las medidas de seguridad de nivel alto.

Artículo 7 Ley 41/2002

"1. Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley.

2. Los centros sanitarios adoptarán las medidas oportunas para garantizar los derechos a que se refiere el apartado anterior, y elaborarán, cuando proceda, las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes."

Para preservar de forma correcta los derechos de los pacientes, con especial referencia a su intimidad, el artículo 16 de la Ley 41/2002 es claro al determinar que "*el acceso a los datos*" debe de realizarse, en todo caso, por un "*profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto*". De igual forma, "*el personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto*". Este deber de secreto unido a la salvaguarda efectiva del derecho fundamental hacen imprescindible el

recurso al cifrado de datos, obligatorio, por otro lado, por el tipo de datos que van a ser tratados y la implantación debida de las medidas de seguridad de nivel alto.

El cifrado de datos es la medida técnica que permite a los centros sanitarios cumplir con su obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad.

Artículos 17.1, 17.5 y 17.6
Ley 41/2002

"1. Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial.

5. Los profesionales sanitarios que desarrollen su actividad de manera individual son responsables de la gestión y de la custodia de la documentación asistencial que generen.

6. Son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal."

El paciente tiene derecho a que los centros sanitarios establezcan un "*mecanismo de custodia activa y diligente de las historias clínicas*" (art. 19 Ley 41/2002). Por tanto, los centros sanitarios tienen la obligación de establecer e implementar dichos mecanismos.

5.4 Código Deontológico de la Abogacía Española

El Código Deontológico de la Abogacía Española establece unas normas deontológicas para la función social de la Abogacía (Preámbulo CDAE), entre las que se encuentra el deber de secreto, que exige el cifrado de datos.

La relación entre el cliente y su abogado se fundamenta en la confianza y exige de este una conducta profesional íntegra, que sea honrada, leal, veraz y diligente. El abogado, "*está obligado a no defraudar la confianza de su cliente*" (art. 4 CDAE).

El deber de secreto, exige el cifrado de datos.

El cliente espera del abogado que guarde secreto profesional sobre todos los datos que le aporte. En algunos casos los datos están relacionados con la real comisión de delitos, de los que salen impunes o por los que se les condena. El cliente deposita su confianza en el abogado sabiendo que este está obligado a no defraudar su confianza, a guardar secreto sobre todos los datos de su vida personal e íntima que le revele y a que esta información permanezca secreta y confidencial para siempre, durante la relación contractual de asesoramiento jurídico y después de esta. Todo el contenido que el cliente revele al abogado tiene que permanecer a resguardo bajo las más altas y estrictas medidas de seguridad, lo que exige el establecimiento de medidas de nivel alto y, por tanto, del cifrado de todos los datos que se encuentren recogidos en formato digital, así como de las comunicaciones que el abogado mantenga con su cliente.

Los derechos con los que trata un abogado son fundamentales y cuentan con la máxima protección constitucional. El de mayor relevancia es el derecho de los clientes "*a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia*" (art. 24 CE).

Artículo 24.2 Constitución Española

"[...] *todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia. [...]*"

La Constitución Española y el CDAE entregan al cliente la seguridad de que su información va a ser guardada con el mayor de los esmeros. Tanto es así, que el deber de confidencialidad del abogado es casi absoluto, además del mayor de los existentes en derecho español. El cliente desnuda su intimidad ante el abogado revelando los detalles de delitos que ha o no ha cometido. Los datos del cliente no pueden trascender en ningún caso.

En muchos casos, los datos que aporta el cliente no son los que la LOPD nomina como sujetos a recibir medidas de seguridad de nivel alto (religión, sexualidad, etc.). Sin embargo, el nivel debe ser siempre el alto, por el tipo de tratamiento y por el máximo riesgo que supone para el cliente en relación con los derechos a no declarar contra sí mismos, a no confesarse culpables, a la presunción de inocencia, a su intimidad, a su honor y a los demás de los regulados en la LO 1/1982 y en la propia CE.

El secreto profesional es un derecho y deber primordial de la Abogacía que merece el mayor de los respetos y que obliga a la implantación de medidas de nivel alto a los ficheros en los que se guarden datos de clientes. Por tanto, todo abogado está obligado al cifrado de, al menos, las carpetas relativas a los casos que lleva. El empleo de gestores online de casos está permitido por la normativa siempre que se respeten y se cumplan las medidas de seguridad de nivel alto;

Artículo 5 CDAE

"**1.** La confianza y confidencialidad en las relaciones entre cliente y abogado, ínsita en el derecho de aquél a su intimidad y a no declarar en su contra, así como en derechos fundamentales de terceros, impone al abogado el deber y le confiere el derecho de guardar secreto respecto de todos los hechos o noticias que conozca por razón de cualquiera de las modalidades de su actuación profesional, sin que pueda ser obligado a declarar sobre los mismos como reconoce el artículo 437.2 de la vigente Ley Orgánica del Poder Judicial.

2. El deber y derecho al secreto profesional del abogado comprende las confidencias y propuestas del cliente, las del adversario, las de los compañeros y todos los hechos y documentos de que haya tenido noticia o haya recibido por razón de cualquiera de las modalidades de su actuación profesional.

3. El abogado no podrá aportar a los tribunales, ni facilitarle a su cliente las cartas, comunicaciones o notas que reciba del abogado de la otra parte, salvo expresa autorización del mismo.

4. Las conversaciones mantenidas con los clientes, los contrarios o sus abogados, de presencia o por cualquier medio telefónico o telemático, no podrán ser grabadas sin previa advertencia y conformidad de todos los intervinientes y en todo caso quedarán amparadas por el secreto profesional.

5. En caso de ejercicio de la abogacía en forma colectiva, el deber de secreto se extenderá frente a los demás componentes del colectivo.

6. En todo caso, el abogado deberá hacer respetar el secreto profesional a su personal y a cualquier otra persona que colabore con él en su actividad profesional.

7. Estos deberes de secreto profesional permanecen incluso después de haber cesado en la prestación de los servicios al cliente, sin que estén limitados en el tiempo.

8. El secreto profesional es un derecho y deber primordial de la Abogacía. En los casos excepcionales de suma gravedad en los que, la obligada preservación del secreto profesional, pudiera causar perjuicios irreparables o flagrantes injusticias, el Decano del Colegio aconsejará al Abogado con la finalidad exclusiva de orientar y, si fuera posible, determinar medios o procedimientos alternativos de solución del problema planteado ponderando los bienes jurídicos en conflicto. Ello no afecta a la libertad del cliente, no sujeto al secreto profesional, pero cuyo consentimiento por sí solo no excusa al Abogado de la preservación del mismo."

esto es, siempre que se cifren los datos tanto en origen como en destino y en la transmisión de los mismos.

5.5 Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (LPBC)

El objeto de la LPBC es proteger "*la integridad del sistema financiero y de otros sectores de actividad económica mediante el establecimiento de obligaciones de prevención del blanqueo de capitales y de la financiación del terrorismo*" (art. 1 LPBC). Esta norma exige la implantación de medidas de seguridad de nivel alto sobre ciertos ficheros que almacenan datos de carácter personal y, en consecuencia, el cifrado de estos.

Esta norma es la que, de forma más directa, muestra qué colectivos de sujetos, tanto personas físicas como jurídicas, están obligados a cifrar datos. **La lista está contenida en el artículo 2 LPBC y alcanza a abogados, profesionales del arte, joyerías, promotores inmobiliarios, servicios postales, entidades de crédito, notarios, y sociedades de garantía recíproca, entre otros muchos.** A continuación los detallamos de manera literal:

Artículo 2.1 LPBC

"*1. La presente Ley será de aplicación a los siguientes sujetos obligados:*
a) Las entidades de crédito.
b) Las entidades aseguradoras autorizadas para operar en el ramo de vida y los corredores de seguros cuando actúen en relación con seguros de vida u otros servicios relacionados con inversiones, con las excepciones que se establezcan reglamentariamente.
c)Las empresas de servicios de inversión.
d) Las sociedades gestoras de instituciones de inversión colectiva y las sociedades de inversión cuya gestión no esté encomendada a una sociedad gestora.
e) Las entidades gestoras de fondos de pensiones.
f) Las sociedades gestoras de entidades de capital-riesgo y las sociedades de capital-riesgo cuya gestión no esté encomendada a una sociedad gestora.
g) Las sociedades de garantía recíproca.
h) Las entidades de pago y las entidades de dinero electrónico.
i) Las personas que ejerzan profesionalmente actividades de cambio de moneda.
j) Los servicios postales respecto de las actividades de giro o transferencia.
k) Las personas dedicadas profesionalmente a la intermediación en la concesión de préstamos o créditos, así como las personas que, sin haber obtenido autorización como establecimientos financieros de crédito, desarrollen profesionalmente alguna de las actividades a que se refiere la Disposición adicional primera de la Ley 3/1994, de 14 de abril, por la que se adapta la legislación española en materia de Entidades de Crédito a la Segunda Directiva de Coordinación Bancaria y se introducen otras modificaciones relativas al Sistema Financiero.
l) Los promotores inmobiliarios y quienes ejerzan profesionalmente actividades de agencia, comisión o intermediación en la compraventa de bienes inmuebles.
m) Los auditores de cuentas, contables externos o asesores fiscales.
n) Los notarios y los registradores de la propiedad, mercantiles y de bienes muebles.
ñ) Los abogados, procuradores u otros profesionales independientes cuando participen en la concepción, realización o asesoramiento de operaciones por cuenta de clientes relativas a la compraventa de bienes inmuebles o entidades comerciales, la gestión de fondos, valores u otros activos, la apertura o gestión de cuentas corrientes, cuentas de ahorros o cuentas de valores, la organización de las aportaciones necesarias para la creación, el funcionamiento o la gestión de empresas o la creación, el funcionamiento o la gestión de fideicomisos («trusts»), sociedades o estructuras análogas, o cuando actúen por cuenta de clientes en cualquier operación financiera o inmobiliaria.
o) Las personas que con carácter profesional y con arreglo a la normativa es-

pecífica que en cada caso sea aplicable presten los siguientes servicios a terceros: constituir sociedades u otras personas jurídicas; ejercer funciones de dirección o secretaría de una sociedad, socio de una asociación o funciones similares en relación con otras personas jurídicas o disponer que otra persona ejerza dichas funciones; facilitar un domicilio social o una dirección comercial, postal, administrativa y otros servicios afines a una sociedad, una asociación o cualquier otro instrumento o persona jurídicos; ejercer funciones de fideicomisario en un fideicomiso («trust») expreso o instrumento jurídico similar o disponer que otra persona ejerza dichas funciones; o ejercer funciones de accionista por cuenta de otra persona, exceptuando las sociedades que coticen en un mercado regulado y estén sujetas a requisitos de información conformes con el derecho comunitario o a normas internacionales equivalentes, o disponer que otra persona ejerza dichas funciones.
p) Los casinos de juego.
q) Las personas que comercien profesionalmente con joyas, piedras o metales preciosos.
r) Las personas que comercien profesionalmente con objetos de arte o antigüedades.
s) Las personas que ejerzan profesionalmente las actividades a que se refiere el artículo 1 de la Ley 43/2007, de 13 de diciembre, de protección de los consumidores en la contratación de bienes con oferta de restitución del precio.
t) Las personas que ejerzan actividades de depósito, custodia o transporte profesional de fondos o medios de pago.
u) Las personas responsables de la gestión, explotación y comercialización de loterías u otros juegos de azar respecto de las operaciones de pago de premios.
v) Las personas físicas que realicen movimientos de medios de pago, en los términos establecidos en el artículo 34.
w) Las personas que comercien profesionalmente con bienes, en los términos establecidos en el artículo 38.
x) Las fundaciones y asociaciones, en los términos establecidos en el artículo 39.
y) Los gestores de sistemas de pago y de compensación y liquidación de valores y productos financieros derivados, así como los gestores de tarjetas de crédito o débito emitidas por otras entidades, en los términos establecidos en el artículo 40.
Se entenderán sujetas a la presente Ley las personas o entidades no residentes que, a través de sucursales o agentes o mediante prestación de servicios sin establecimiento permanente, desarrollen en España actividades de igual naturaleza a las de las personas o entidades citadas en los párrafos anteriores."

El motivo por el que todos estos sujetos están obligados al cifrado de determinada información lo encontramos en dos artículos de la LPBC:

1.Los sujetos obligados "*aplicarán medidas reforzadas de diligencia debida*" en las relaciones de negocio u operaciones de personas con responsabilidad pública (art. 14 LPBC). Estos sujetos obligados podrán proceder a la creación de ficheros donde se contengan los datos identificativos de las personas con responsabilidad pública. "*En todo caso deberán implantarse sobre el fichero las medidas de seguridad de nivel alto*", que exige el cifrado de los datos (art. 15 LPBC).

2.El tratamiento de datos de carácter personal, así como los ficheros, automatizados o no, creados para el cumplimiento de las disposiciones de toda la LPBC se someterán a lo dispuesto en la LOPD. Además, "*serán de aplicación a estos ficheros las medidas de seguridad de nivel alto*", que exigen el cifrado de datos (art. 32 LPBC).

Un extraordinario número de sujetos está obligado a cifrar datos de forma legalmente correcta por así disponerlo la LPBC, la LOPD y su normativa de desarrollo. Además, como todos los sujetos

que tratan datos personales y han tenido que implantar medidas a partir del nivel medio, siendo este nivel alto, deberán someter los sistemas de información e instalaciones de tratamiento y almacenamiento de datos, "*al menos cada dos años, a una auditoría interna o externa*" (art. 96 RLOPD) en la que se verificará que el cifrado es correcto y acorde a lo exigido por la normativa.

5.6 Esquema Nacional de Seguridad (ENS)

La finalidad del Esquema Nacional de Seguridad o ENS es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. Este ENS fue aprobado por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Este esquema es aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

El ENS hace referencia en varias secciones a la conveniencia o necesidad de cifrar tanto la información como las comunicaciones. Además especifica medidas concretas de seguimiento obligatorio tanto para el uso de criptografía en las comunicaciones, como para el uso de criptografía en los soportes de información.

Estas son algunas de las principales indicaciones del cifrado en el ENS:

- Un cifrado débil es un cifrado inseguro: "*Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil*" (art. 21 ENS).
- Protección de portátiles: "*La información de nivel alto almacenada en el disco se protegerá mediante cifrado*" (5.3.3 Anexo II ENS).
- Solo se verá en claro la información en uso: "*La información con un nivel alto en confidencialidad se cifrará tanto durante su almacenamiento como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella*" (5.7.3 ENS).
- Se deben cifrar las copias de respaldo: "*Las copias de respaldo disfrutarán de la misma seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad de que las copias de seguridad estén cifradas para garantizar la confidencialidad*" (5.7.7 Anexo II ENS)

Por medio del cifrado, el ENS sustenta ciertos principios básicos y requisitos mínimos requeridos para una protección adecuada de la información.

6 Cifra el contenido que subes a Dropbox

Los sujetos obligados deben cifrar determinados contenidos que suben a Dropbox, así como los que guardan o tratan en otros sistemas de Cloud Computing.

El Cloud Computing es "*un modelo de prestación de servicios tecnológicos que permite el acceso bajo demanda y a través de la red a un conjunto de recursos compartidos y configurables (como redes, servidores, capacidad de almacenamiento, aplicaciones y servicios) que pueden ser rápidamente asignados y liberados con una mínima gestión por parte del proveedor de servicios*", según el Informe 'Utilización del Cloud Computing por los despachos de abogados y el derecho a la protección de datos de carácter personal' de la Agencia Española de Protección de Datos y el Consejo General de la Abogacía Española, que toma como base la definición ofrecida por The NIST Definition of Cloud Computing.

Siempre que vaya a hacer uso de un sistema de cloud computing, el cifrado de los datos personales es "*una medida que debe valorarse positivamente*", según la Agencia Española de Protección de Datos, como respuesta a la pregunta "*¿Cómo puedo garantizar o asegurarme de que se cumplen las medidas de seguridad?*", en la 'Guía para clientes que contraten servicios de Cloud Computing'. La AEPD sugiere que se solicite información al proveedor de cloud sobre el cifrado de los datos en todos los casos, no solo en los que haya que cumplir con las medidas de seguridad de nivel alto.

Para la AEPD, en la Guía para clientes que contraten servicios de Cloud Computing, ante la pregunta, un elemento de la seguridad cobra especial relevancia en un entorno 'cloud' es la "*aplicación de técnicas robustas de cifrado tanto a los datos en tránsito como a los datos almacenados*", ya que constituye una medida necesaria para garantizar su confidencialidad.

En relación con las profesiones que exigen secreto profesional y siempre que las medidas de seguridad a aplicar en materia de protección de datos sean de nivel alto, "*el cifrado de datos almacenados es una necesaria medida de seguridad*", según se apunta en el Informe 'Utilización del Cloud Computing por los despachos de abogados y el derecho a la protección de datos de carácter personal. El proveedor ha de dar a conocer "*el nivel de seguridad ofrecido por las técnicas de cifrado de la información que aplique en sus sistemas*", si es que aplica alguno. A continuación se ha verificar que realmente el nivel es el adecuado para cumplir la normativa aplicable. Si no lo fuera o ante la duda, habrá que tomar una de estas dos opciones: cambiar de prestador de servicios de cloud computing o aplicar un cifrado adecuado propio o de un prestador externo.

En servicios de cloud computing, el cifrado de datos es del todo esencial y obligatorio para los sujetos obligados por la normativa a aplicar medidas de nivel alto. Asimismo, también es obligatorio para todos aquellos colectivos que deban guardar secreto profesional.

7 Más motivos para cifrar

Cifrar siempre es conveniente, aunque no haya ninguna ley que obligue a ello. Un número elevado de sujetos están obligados a cifrar por las ventajas que conlleva en materia de seguridad y confidencialidad. En el resto de casos, cifrar es de utilidad extraordinaria ya que refuerza la seguridad, genera confianza y evita situaciones comprometidas en los tribunales.

7.1 Protección de la propiedad intelectual

Los productores, los creativos, los publicistas y todos los autores en general deben velar por su trabajo en todo momento. Cuando la obra está inacabada o aún no está lista para su divulgación (art. 4 LPI), los autores pueden cifrar su contenido con el objetivo de que sean solo ellos quienes puedan acceder al mismo.

Artículo 4 Ley de Propiedad Intelectual

"A efectos de lo dispuesto en la presente Ley, se entiende por divulgación de una obra toda expresión de la misma que, con el consentimiento del autor, la haga accesible por primera vez al público en cualquier forma; y por publicación, la divulgación que se realice mediante la puesta a disposición del público de un número de ejemplares de la obra que satisfaga razonablemente sus necesidades estimadas de acuerdo con la naturaleza y finalidad de la misma."

La propiedad intelectual de una obra literaria, artística o científica corresponde al autor por el solo hecho de su creación, sin que sea preciso un registro (art. 1 LPI). El cifrado de los contenidos hace posible que el autor controle en todo momento el destino de su creación.

7.2 Protección de los secretos comerciales

Las meras ideas cuentan con una protección legal un tanto indefinida. El cifrado es la solución para que estos secretos, confidenciales, puedan permanecer a la vista de unos pocos privilegiados y ocultos para la sociedad en general.

La divulgación o explotación, sin autorización de su titular, de secretos industriales o de cualquier otra especie de secretos empresariales a los que se haya tenido acceso legítimamente, pero con deber de reserva, o ilegítimamente se consideran desleales (art. 13 LCD). Sin embargo, el problema no es si son o no desleales estas conductas, sino que las acciones legales que puedan ejercitarse contra los infractores solo tienen cabida cuando el daño se ha producido; esto es, en materia de secreto comercial, la norma solo protege después de que se hayan divulgado o explotado los secretos. La persecución de las violaciones de secretos precisa que la violación haya sido efectuada con ánimo de obtener provecho, propio o de un tercero, o de perjudicar al titular del secreto, con lo que la acción se hace aún más complicada.

Artículo 13 de la Competencia Desleal

"1. Se considera desleal la divulgación o explotación, sin autorización de su titular, de secretos industriales o de cualquier otra especie de secretos empresariales a los que se haya tenido acceso legítimamente, pero con deber de reserva, o ilegítimamente, a consecuencia de alguna de las conductas previstas en el apartado siguiente o en el artículo 14.
2. Tendrán asimismo la consideración de desleal la adquisición de secretos por medio de espionaje o procedimiento análogo.
3. La persecución de las violaciones de secretos contempladas en los apartados anteriores no precisa de la concurrencia de los requisitos establecidos en el artículo 2. No obstante, será preciso que la violación haya sido efectuada con ánimo de obtener provecho, propio o de un tercero, o de perjudicar al titular del secreto."

La solución para proteger los secretos comerciales es el cifrado. Cifrando los datos se dificulta la divulgación y a la explotación no autorizada de secretos comerciales, así como la adquisición de secretos por medio de espionaje o procedimiento análogo.

7.3 Protección contra el espionaje industrial

El cifrado ayuda evitar que la empresa pise los Tribunales de lo Penal.

La comisión de delitos relativos al mercado y los consumidores es, en la era de la tecnología, cada vez más frecuente. Con un mecanismo de cifrado ade-

cuado se consiguen minimizar los ataques exitosos ya que todo lo que verá el intruso es un conjunto de información ininteligible que será incapaz de manipular.

Un sistema adecuado de protección de datos es el que complementa el factor humano con medidas de tipo técnico, tales como el cifrado, el bloqueo de puertos, la imposibilidad de instalar software no autorizado en equipos corporativos...

Los ataques pueden venir de fuera o proceder de dentro de la empresa. Hasta 5 años de prisión para el atacante, además de otras penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos, es una consecuencia fatal para el autor. La justicia tendrá efectos. Pero el daño se pudo haber evitado tomando las medidas técnicas y humanas adecuadas. Un sistema de cifrado completo, sencillo y conforme a los requisitos legales (art. 104 RLOPD) es la mejor barrera para salvar el obstáculo penal y hacer que la empresa se construya sobre pilares seguros.

Con el cifrado, evitarás tener que leer de nuevo estos artículos:

Artículo 278 del Código Penal

"1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos."

Artículo 279 del Código Penal

"La difusión, revelación o cesión de un secreto de empresa llevada a cabo por quien tuviere legal o contractualmente obligación de guardar reserva, se castigará con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses."

La mejor protección siempre es un buen cifrado.

7.4 Protección para aceptar BYOD (Bring Your Own Device)

La tendencia empresarial es el BYOD (Bring Your Own Device) o "Trae tu propio dispositivo". Esta práctica implica una cantidad ingente de riesgos en relación con la protección de la información en todos sus niveles: datos personales, creaciones, secretos comerciales...

INTECO, el Instituto Nacional de Tecnologías de la Comunicación, recomienda a las compañías que apuesten por el BYOD que conciencien al empleado, "*para que en caso de que este lo use para temas de trabajo, incorpore las mismas medidas de seguridad que los dispositivos utilizados dentro de la compañía*". Asimismo, ofrece una recomendación clara en cuanto al cifrado de datos en su artículo 'Móviles personales y otros « wearables » en la empresa: los riesgos del BYOD': "*No permitir el almacenamiento de información sensible dentro del dispositivo. Y en caso de que se produzca recomendar el uso de cifrado.*"

La normativa obliga a aplicar cifrados en los dispositivos de los empleados, en las áreas que admitan BYOD de todas las empresas que tienen obligación de cifrar alguno de sus ficheros, siempre que el trabajador vaya a almacenar o tratar dicha información. Las empresas que desean proteger determinados archivos deben también cifrar los dispositivos de los empleados que tengan acceso a los mismos.

El riesgo de del BYOD es extremo en materia de seguridad. El empleado puede: extraviar el dispositivo, permitir que lo utilicen familiares o amigos, olvidar cam-

biar la contraseña de acceso, conectarse a través de una red 2G permitiendo la extracción de datos, enchufar su equipo a un cargador USB falso en un bar, instalar malware que envía archivos al exterior o, simplemente, anclar su dispositivo a una red 4G ajena a la propia de la compañía para realizar a través de ella lo que a través de la red de la compañía no podría.

El CERT Gubernamental español (CNN-CERT), que forma parte del Centro Nacional de Inteligencia (CNI), realizó una encuesta a empleados BYOD. Según el CERT, *"el dato más preocupante es que cerca de la mitad de los encuestados no manejan la información corporativa de forma cifrada en su dispositivo personal, incluso el 15,6% dice no saber cómo se debe manejar dicha información"* ('Riesgos y amenazas del Bring Your Own Device (BYOD)'). El CERT señala que este tipo de trabajadores puede conectarse a redes que desconocen que son inseguras, posibilitando "*ciberataques de tipo man-in-the-middle, que podrían interceptar e incluso modificar los datos en tránsito*". Para evitar esta consecuencia, la primera medida de seguridad que recomienda que el CERT adoptar es "usar mecanismos de cifrado fuerte", tales como el uso de redes privadas virtuales VPN con el refuerzo de un sistema propio y eficaz de cifrado de datos.

Dentro del análisis de riesgos que el CERT realiza en su informe sobre BYOD, indica un aspecto que convendría tener en cuenta: La "*seguridad jurídica en caso de pérdida, robo o finalización de la relación de trabajo del empleado, requiriendo el uso de contraseñas de acceso, bloqueo de dispositivos, cifrado de información, así como el derecho institucional a borrar remotamente los datos corporativos del equipo*". El cifrado de la información vuelve a resultar una medida esencial.

Resulta extremadamente recomendable llevar a cabo un cifrado completo de todos los dispositivos del empleado que vayan a ser utilizados también para el trabajo, además de configurar medidas que le permitan abrir determinados archivos, le impidan enviar otros o le bloqueen el borrado o la edición del resto.

7.5 Protección adicional para generar seguridad

Determinadas empresas que no tienen la obligación de cifrar eligen hacerlo para trabajar bajo el amparo de su seguridad. Estas empresas protegen su información frente a terceros bajo un velo de opacidad, lo que hace el manejo y la transmisión de información sea más ágil y sencilla.

Las empresas pueden elegir cumplir los "*mínimos exigibles*" (art. 81.7 RLOPD) que marca la normativa de protección de datos o pueden dotar a sus procesos de mayor seguridad y confidencialidad. Cuando una corporación usa datos y realiza tratamientos de nivel bajo y medio puede optar por asegurar la información por medio del cifrado.

El Gabinete Jurídico de la Agencia Española de Protección de Datos afirma, en el Informe 0477/2009, que, aun cuando no sea imperativa, "*la medida de cifrado de los datos puede ser adoptada voluntariamente por el responsable del fichero*" para superar los mínimos exigibles marcados por la norma.

8 Libertades y precauciones sobre el cifrado

Es posible llevar a cabo un cifrado selectivo de datos, así como otorgar permisos de acceso a determinados usuarios individualizados o a grupos de trabajadores, de manera que la empresa tenga una capacidad completa de control sobre la información a la que cada usuario tiene acceso.

8.1 Cifrado selectivo

Las empresas pueden decidir aplicar el sistema de cifrado solo a una sección de los datos que alberga en un mismo fichero. Conforme a lo previsto en el artículo 81.8 del Reglamento, puede segregar el fichero, aplicando el cifrado únicamente a los datos que considere. Este tipo de segregación puede realizarse en ficheros que contengan una gran variedad de datos entre los que se encuentren datos de, por ejemplo, salud o raza. Las medidas de seguridad de nivel alto pueden aplicarse únicamente a los datos de tal carácter.

Artículo 81.8 RLOPD

"A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad."

8.2 Otorga o restringe el acceso a los distintos empleados

Si la empresa adopta el sistema de cifrado de forma voluntaria para contenidos que no alberguen datos personales, podrá prescindir de otras medidas como, por ejemplo, el control de accesos o la identificación y la autenticación. En cambio, si desea aplicar estas medidas o siempre que los ficheros contengan datos personales, tendrá que tener en cuenta una serie de medidas adicionales al propio cifrado como adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios y establecer mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

Un sistema de cifrado adecuado que se quiera aplicar a un conjunto de datos que vaya a ser accedido por una pluralidad de personas debe permitir al administrador dotar de derechos de descifrado a algunos usuarios o a determinados grupos de usuarios (por ejemplo, al departamento de recursos humanos o al de marketing) y negar el acceso al resto. Además, debe poder segmentar los tipos de ficheros, de manera que una determinada parte de ellos estén disponibles a ciertos usuarios. Una opción extraordinaria de cifrado es la de clave compartida, que permite a más de un empleado acceder a cierta información.

Cuando la normativa lo exige es imprescindible que se adopte una serie de medidas adicionales a la del cifrado, cuales son las de identificar a los usuarios, autentificarlos, conocer la cantidad de intentos que han realizado poniendo su contraseña para acceder a la documentación y bloquear el acceso cuando se sobrepase una determinada cifra y conocer si han realizado modificaciones sobre la información, entre otros. Cada caso es diferente y deberá analizarse la conveniencia de implantar unas u otras medidas con objeto de cumplir plenamente la normativa.

A continuación indicamos las principales necesidades básicas en cuanto a acceso a recursos e identificación y autenticación de usuarios, que pueden ser aplicadas a través de un solo sistema de cifrado o de varias herramientas conjuntas.

Artículo 91 RLOPD

"1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio."

Artículo 93 RLOPD

"1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.
3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las c ontraseñas que, mientras estén vigentes, se a lmacenarán de forma ininteligible."

En el nivel medio, esta medida de identificación y autenticación se vuelve más rigurosa ya que, a las medidas anteriores previstas para el nivel básico, se añade la contenida en el artículo 98 RLPOD según el cual "*el responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.*"

Por último, en el nivel alto, se requiere ya un registro de cada intento de acceso que se produzca, establece el artículo 103.1 RLOPD que "*de cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.*" Mientras que el número segundo del mismo artículo dispone "*En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.*"

El cifrado de los datos se puede realizar sin excesiva dificultad, con un coste razonable y con la seguridad de que se cumple la ley de forma adecuada. La mayoría de las herramientas de cifrado profesional son modulares o permiten la gestión completa a través de un panel de control específico.

Ahora, generar un búnker legal de uso sencillo aplicando tecnologías completas de cifrado es posible.

ABANLEX

Despacho de abogados
con especialización en
tecnología y protección de datos.

Resolver casos complejos de Derecho Tecnológico es la principal función de Abanlex, despacho de abogados especializado en la protección de la información, la privacidad y la innovación jurídica. Los abogados de Abanlex permanecen en la vanguardia de los movimientos legislativos, colaborando en la elaboración de aquellos que tocan sus áreas de ejercicio.

Las soluciones que ha ejecutado para resolver casos de extraordinaria complejidad sitúan a Abanlex como un despacho de referencia internacional en diferentes materias como los nuevos sistemas electrónicos de pago, los sistemas de cifrado o los dispositivos de seguimiento. Sus últimos casos de relevancia internacional son: el Derecho al Olvido contra Google, que ha llevado ante el TJUE y ahora dirige ante la Audiencia Nacional, y los avances en criptomonedas, que le ha valido citas en varios documentos del Gobierno de España y del de Estados Unidos.

Abanlex tiene su sede en Madrid, España. Más información disponible en www.abanlex.com

Abanlex. c/ Velázquez, 109, 7ª Planta. 28006 Madrid. Correo electrónico: info@abanlex.com (@abanlex)

SOPHOS

Lider en el
Cuadrante Mágico de Gartner
de protección de datos móviles.

Más de 100 millones de usuarios en 150 países confían en las soluciones de seguridad completa de Sophos como la mejor protección contra amenazas complejas y fuga de datos. De fácil despliegue, administración y uso, las premiadas soluciones para la protección de estaciones de trabajo, web, email, móvil, cifrado y seguridad de red ofrecidas por Sophos, están respaldadas por SophosLabs, una red global de centros de investigación de amenazas.

Sophos ofrece seguridad completa protegiendo todos los puntos, desde la red a los servidores, pasando por las estaciones de trabajo y los dispositivos móviles. Gracias estas soluciones, las empresas podrán concentrarse en las necesidades de su negocio.

Sophos tiene su sede en Boston, EE.UU. y Oxford, Reino Unido. Más información disponible en www.sophos.com/es-es .
Sophos Iberia. c/Orense, 81 1ª Planta. 28020 Madrid. ComercialES@sophos.com (@sophosiberia)
Telf.: 913 756 756